(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) **EP 2 033 112 B1**

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
20.12.2017 Bulletin 2017/51

(21) Application number: **07795324.8**

(22) Date of filing: **25.05.2007**

(51) Int Cl.:
H04L 12/24 *(2006.01)* ***G07F 19/00*** *(2006.01)*
G06F 15/173 *(2006.01)* ***H04L 12/26*** *(2006.01)*
H04L 29/06 *(2006.01)* ***H04L 29/08*** *(2006.01)*

(86) International application number:
PCT/US2007/012449

(87) International publication number:
WO 2008/097245 (14.08.2008 Gazette 2008/33)

(54) **IMPROVED NETWORK MANAGEMENT**

VERBESSERTES NETZWERKMANAGEMENT

GESTION DE RÉSEAU AMÉLIORÉE

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IS IT LI LT LU LV MC MT NL PL PT RO SE SI SK TR

(30) Priority: **06.02.2007 US 702852**
06.02.2007 US 703028
06.02.2007 US 702986
26.05.2006 US 808866 P

(43) Date of publication of application:
11.03.2009 Bulletin 2009/11

(73) Proprietor: **The PNC Financial Services Group, Inc.**
Pittsburgh, PA 15222 (US)

(72) Inventors:
- **KOMLENIC, Todd**
  Beaver, PA 15009 (US)
- **HOUSEHOLDER, David**
  Beaver Falls, PA 15010 (US)
- **THARP, Thomas**
  Pittsburgh, PA 15234 (US)

(74) Representative: **Gill Jennings & Every LLP**
The Broadgate Tower
20 Primrose Street
London EC2A 2ES (GB)

(56) References cited:
EP-A2- 0 455 402
US-A- 5 592 620
US-A- 5 651 006
US-A1- 2001 052 006
US-A1- 2002 083 166
US-A1- 2004 047 324
US-A1- 2004 199 626
US-A1- 2004 249 973
US-A1- 2006 071 776
US-B1- 6 229 807
US-B1- 6 292 472
US-B1- 6 490 617
US-B1- 7 036 048

Note: Within nine months of the publication of the mention of the grant of the European patent in the European Patent Bulletin, any person may give notice to the European Patent Office of opposition to that patent, in accordance with the Implementing Regulations. Notice of opposition shall not be deemed to have been filed until the opposition fee has been paid. (Art. 99(1) European Patent Convention).

EP 2 033 112 B1

Description

BACKGROUND

[0001] In many computer networks, it is desirable to monitor the status of network agents. For example, a bank having a network of Automated Teller Machines (ATM's) needs to know the status of its ATM's. In the same way, other network operators having remote agents often need to manage their agents for similar reasons. Most of the existing methods for managing networks rely primarily on active polling or pinging of agents. According to these methods, a host machine or machines on the network periodically polls each agent on the network. When an agent receives a poll or ping, it prepares and sends a response message to the host. The host verifies the status of an agent based on whether it replies to the poll and on status data that may be included in the response message. If more information about the status of an agent is required, for example, if the response message indicates a problem, additional pings or polls may be sent to the agent.

[0002] Although active maintenance systems can be effective, they also have certain drawbacks. For example, active maintenance requires a great deal of bandwidth. For every poll or ping to an agent, two messages are carried on the network: the poll or ping and the response message. Bandwidth-related concerns can be particularly troublesome when all or a portion of the network path between a host and an agent is bandwidth limited, or rented on the basis of bandwidth, in addition to its bandwidth issues, active maintenance also is incapable of managing agents that the host does not know about. Each ping or poll made by the host must be directed to the address of an agent. If the host is unaware of any agents on the network, it most likely does not know those agents' addresses and cannot ping or learn anything about them.

[0003] EP0455402A2 describes a computer network node discovery system that provides a general way of discovering network elements, on nodes, connected to a computer network.

[0004] US005651006A describes a hierarchical communication network management system structured by a plurality of agents and sub-managers connected to lower communication networks and an integration manager connected to a higher communication network.

[0005] US007036048B1 describes a fault monitoring and notification system for automated banking machines operating in a network. Status messages generated by the banking machines are stored and subsequently processed to resolve an action to be taken in response to the messages.

SUMMARY

[0006] In one general aspect, the present invention is directed to a method of managing a network comprising a plurality of agents according to appended claim 1. The method may comprise the step of storing a plurality of agent data files corresponding to the plurality of agents. Upon receiving a status message from a first agent, the method may comprise the step of updating an agent data file corresponding to the first agent. Also, the methods may comprise the steps of periodically identifying agent data files from the plurality of agent data files that have not been updated for a predetermined amount of time; and sending a request for response to a second agent corresponding to an agent data file that has not been updated for a predetermined amount of time.

[0007] In another general aspect, the present invention is directed to a computer system according to appended claim 9.

[0008] In yet another general aspect, the invention is directed to a computer readable medium according to appended claim 17.

FIGURES

[0009] Various embodiments of the present invention are described here by way of example in conjunction with the following figures, wherein:

Figure 1 shows a diagram of a network according to various embodiments;
Figures 2-3 show diagrams of network components according to various embodiments;
Figures 4-5 show process flows according to various embodiments;
Figures 6, 6A, 7-9, 9 A and 9B show screen shots of a user interface according to various embodiments; and
Figure 10 shows a process flow according to various embodiments.

DESCRIPTION

[0010] Figure 1 shows an exemplary network 100 according to various embodiments. The network 100 may facilitate communication between a host 102 and one or more remote agents 104. The network 100 itself may comprise a proprietary network 106 and various remote networks 108, 110. The proprietary network 106 may include network hardware (*e.g.,* servers, routers, cabling, *etc.*) that is owned and/or maintained by the individual or organization implementing the network 100 (*e.g.,* a bank or other organization). Components may be connected to the proprietary network 106 according to any suitable wired or wireless method. For example, some components of the wireless network 106 may be connected via connections directly owned or administered by the network administrator while other components may be connected to the network 106 via leased connections provided by a third party. The remote networks 108, 110 may include commercial networks or network access services that allow machines on the proprietary network

106 to access machines beyond the proprietary network 106, (*e.g.,* some agents 104). For example, the remote networks 108, 110 may include the networks of Internet service providers (ISP's), cellular service providers, *etc.* Access to the remote networks 108, 110 may be purchased, for example, in units of bandwidth, time, periodic access fees, *etc.* In Figure 1, remote network 108 is represented as a wired network and remote network 110 is represented as a wireless network. It will be appreciated that remote networks that are mixed wired/wireless networks may also be utilized.

[0011] Communication between the host 102 and the agents 104 may be handled by some combination of the proprietary network 106 and the remote networks 108, 110. For example, the host 102 may be able to communicate directly with agents 104 that are resident on the proprietary network 106. For agents 104 that are not resident on the proprietary network 106, the host 102 may be in contact via one or more of the remote networks 108, 110. The proprietary network 106 may be in communication with the remote networks 108, 110, via routers 112, 114, 116. The routers 116 may represent the hardware on the proprietary network 106 where encrypted communications to components on the network 106 terminate. Although the routers 106 are shown at the edge of the proprietary network 106, it will be appreciated that that they may be physically positioned at any point in the network 106.

[0012] Figure 2 shows an exemplary diagram, according to various embodiments, of a host 102. The host 102 may include various software modules including a passive module 202, an active module 204, a cryptographic module 206, and a statistics module 208. The functions of the various modules will be described in more detail below. A host data store 210 may be used to store various information related to the network 100 including the agent data files described below. Also, according to various embodiments, the host 102 may provide a user interface 212 to a user 214. The user 214 may be any kind of user including, an administrative user charged with maintaining the network 100 or a portion thereof, a customer or end user, *etc.* The user interface 212 may allow the user 214 to monitor and/or manipulate the management of the network, for example, as described in more detail below. According to various embodiments, access to the interface 212 may be restricted to credentialed administrative users. The interface 212 may be provided while the user 214 is directly accessing a machine that includes all or part of the host 102, or may be accessed remotely (*e.g.*, from an agent 104). It will be appreciated that the host 102 may be implemented across one or more individual machines.

[0013] Figure 3 shows an exemplary diagram, according to various embodiments, of an agent 104. The agent 104 may include various components including, for example, a modem 302, a associated device 304 and an agent data store 306. The modem 302 may allow the agent 104 to communicate on the network 100 via the proprietary network 106, the wired remote network 108, and/or the wireless remote network 110. For example, if the agent 104 is intended to communicate on a wireless network, the modem 302 may include a wireless modem such as a MULTI-SERVICE MODEM (MSM Series) modem available from GLOBAL NET COMMERCE INC. Likewise, if the agent 104 is intended to communicate on a wired network the modem 302 may include an Ethernet or other wired network interface card or unit. Also, the modem 302 may be programmed with various parameters necessary to communicate on the network 100, including the proprietary network 106 and any applicable remote networks 108, 110. For example, the modem 302 may be programmed with various encryption keys, network addresses, *etc.*

[0014] The associated device 304 may be any type of device that serves a useful purpose on the network 100. For example, when the proprietor of the network 100 is a bank, the associated device 304 may be an ATM. According to other various embodiments, the associated device 304 may be an e-mail kiosk, parking pay-station, remote ticket distributor, *etc.* An agent data store 306 may be used to store various data about the agent 104 including, for example, data related to the agent's connectivity on the network 100, data related to the functionality of the associated device 304, *etc.* According to various embodiments, the agent 104 may provide a user interface 308 to a user 214. The interface 308 may serve various purposes. For example, the interface 308 may allow the user 214 to troubleshoot problems with the agent 104. In addition, the interface 308 may allow the user 214 access to services provided by the associated device 304 (*e.g.,* banking services, vending services, *etc.*).

[0015] According to various embodiments, each agent 104 may be configured to send an unsolicited status message or trap to the host 102 at a given interval (*e.g.*, every 5 minutes). This may be accomplished according to various methods. For example, some agents 104 may include dedicated processors that send the periodic status messages. Some agents 104 may also include modems 302 that can be configured to send periodic status messages by manipulating the modem's firmware settings. The status messages themselves may be configured according to any suitable communication protocol including, for example, Simple Network Management Protocol (SNMP). Status messages may include a name of an agent 104 and/or another identifiable indication that the particular agent 104 is active. According to various embodiments, the status messages may also include information about the status of an agent 104. For example, in an embodiment where the agent is configured to operate on a wireless network, a status message may include an indication of Received Signal Strength Indication (RSSI), pilot signal to interference ratio (E_C/I_O), channel, Ethernet status, *etc.* Where the agent is configured to operate on a wired network, status messages may include various other status information about wired con-

nections including, Ethernet status, *etc.*

[0016] Figure 4 shows a process flow 400, according to various embodiments, for passively managing agents 104 on the network 100. At step 402, the host 102 may receive periodic status messages from agents 104 on the network 100. According to various embodiments, the host 102 (*e.g.*, via the passive module 202) may maintain a log or data file for each configured agent 104 (*e.g.* at host data storage 210). The data file may include a record of status messages received from a corresponding agent and an indication of any status information included in the messages. The agent data files may be created manually when an agent 104 is set up on the network, or may be created automatically by the host 102 when a first status message is received from an agent. At step 404, the host 102 (*e.g.,* the passive module 202) may update the agent data files based on received status messages. It will be appreciated that steps 402 and 404 may be performed continuously and/or simultaneously as status messages are received by the host 102.

[0017] At step 406, the host 102 (*e.g.,* via the passive module 202) may make periodic checks of all of the agent data files to determine if any agent data files are stale. The periodic checks of agent data files may be made at any suitable time interval including, for example, every two minutes. An agent data file may be stale if the host 102 has not received a status message from the agent 104 within a given time period (*e.g.*, ten minutes). If any agent data files are stale at decision step 408, then the status of agents 104 with stale data files (*e.g.,* stale agents) maybe verified at step 410 (*e.g.,* by the active module 207 of the host 102). The host 102 may verify the status of a stale agent 104 according to any suitable method or test. For example, the host 102 may actively ping the agent 104 for a predetermined amount of time. Also, in various embodiments, the host 102 may attempt to initiate a Trivial File Transfer Protocol (TFTP), telnet or other session with the host 102.

[0018] If the host is able to verify that an agent 104 is active, then the host's data file may no longer be considered stale. If the host 102 is unable to verify that an agent 104 is active, then that agent may be placed in a default list at step 414. The default list, which may be stored, for example, at the host data store 210, may indicate agents 104 that are not active or are experiencing communication problems. According to various embodiments, certain agents 104 maybe added to the default list even if the host 102 is able to verify that they are active. For example, if a particular agent 104 has failed to send status messages at the proper interval more than a predetermined number of times, or more than a predetermined number of times over a given time period, then it may be considered in default even if it responds to a ping or other activity test. Also, agents 104 that have a status parameter or parameters outside of predetermined thresholds, as described below, may be added to the default list. The default list may be stored, for example, at host data store 210. According to various embodiments, the host 102 may present the default list to a user 214, for example, via user interface 212.

[0019] It will be appreciated that according to the process flow 400, status messages may be generated and sent by the agents 104 automatically, without any active pings or polls from the host 102. Active pings or polls may be sent by the host 102 when it has failed to receive appropriate status messages from an agent 104. Accordingly, the volume of communication on the network 100 and consequently the bandwidth requirements may be less than that of traditional poll-based methods. Also, as shown by Figure 1, communications between the host 102 and many of the agents 104 may traverse the remote networks 108 and 110. Because access to these remote networks 108, 110 is often purchased based on bandwidth, the reduced bandwidth of the method may result in substantial cost savings. Also, the reduced bandwidth may facilitate wireless connections in the network path, where excessive bandwidth may be unavailable or very expensive.

[0020] In addition to monitoring the status of agents 104 that are configured to send periodic status messages, the host 102 may also detect all agents 104 that are communicating across the proprietary network 106. According to various embodiments, communications on the network 100 may be encrypted. For example, portions of the network 100 may be publicly accessible (*e.g.*, remote networks 106, 110) and/or connected to the Internet. As a result, devices other than those authorized to communicate on the network 100 may be in contact with network devices. Encryption may allow network devices to communicate with one another securely without interference from other devices. For example, only agents 104 or hosts 102 having proper cryptographic keys may be able to send and receive secure communications.

[0021] Figure 5 shows a process flow 500 for detecting agents 104 that are active on the network 100, including agents 104 that are not configured to send periodic status messages. At step 502, the host 102 (*e.g.*, via the cryptographic module 206) may find the current cryptographic associations of the network 100. This may be accomplished by polling the proprietary network routers 116. In response, the routers 116 may provide a list of all agents 104 that have passed an encrypted communication through one or more of the routers 116 over a given time period (*e.g.*, cryptographic associations). The cryptographic associations may include various information about the agents 104 including, for example, their public and private Internet Protocol (IP) addresses, the number of encrypted packets sent and/or received, the subnet mask, *etc.* It will be appreciated that the proprietary network routers 116 may facilitate communication with the remote networks 108, 110 as well as with any agents 104 present on the proprietary network 106. Accordingly, any agent 104 communication directed to any device on the proprietary network 106 may pass through at least one of the routers 116. As a result, the list of cryptographic associations may be a good indication of all of the agents

104 that are active on the network 100.

[0022] Referring back to the process flow 500, at step 504, the host 102 (*e.g.,* via the cryptographic module 206) may match the cryptographic associations with known agents 104 that are sending periodic status messages (*e.g.*, those agents 104 that have an active agent data file). According to various embodiments, cryptographic association data may be organized by public and private IP addresses, while the agent data files may be kept based on agent names. Accordingly, matching cryptographic associations with agent data files may involve the use of Domain Name Server (DNS) functionality to convert IP addresses to their corresponding agent names or visa versa. It will be appreciated that the DNS functionality may be configured to translate IP addresses to agent names, and/or to translate agent names to IP addresses.

[0023] There may be some agents 104 on the network that are not configured to send periodic status messages and/or do not have an active agent data file. These agents 104 may not have a name associated with their IP address(es). If any such agents are found at decision step 506, then they may be added to a pending list at step 508. The pending list may include a listing of all agents 104 that are active on the network 100, but are not sending periodic status messages as described above. The pending list may be provided to a user 214, for example, via user interface 212. The user 214 may utilize the pending list to prepare and/or configure agents 104, for example, as described below. According to various embodiments, an agent 104 may be automatically removed from the pending list when the host 102 receives a first status message from the agent 104.

[0024] Figures 6, 6A, 7-9, 9A and 9B show shots of a series of screens that may be provided to a user 214 via the user interface 212. Figure 6 shows a view of a screen 600 configured to display information regarding all agents 104 that are sending periodic status messages. It will be appreciated that the screen 600 may be arranged according to any suitable configuration. For example, as shown in Figure 6, the screen 600 is arranged into a series of columns and rows with each row corresponding to a single agent 104 and each column including a piece of information about the agents 104.

[0025] Column 602 lists agent names. Column 604 lists the date and time when the most recent status message was received from each agent 104. Column 606 may show the public IP address of each agent 104. Another embodiment of the screen 600, shown in Figure 6A, includes an additional column 609 for the private IP address of the agents 104. Referring back to Figure 6, columns 610 and 612 may list addresses, states and zip codes indicating agent 104 locations. It will be appreciated that these fields may be omitted for agents 104 that are not at a fixed location. Column 614 may list agent 104 phone numbers. An agent 104 may have a phone number, for example, when it is configured to communicate on a wireless remote network, such as 108, and the wireless remote network is a cellular service provider. The phone number may represent an agent's address on the remote network. Columns 616, 618, 620 and 622 may show various status information included in status messages received from the agents 104 including, for example, Received Signal Strength Indication (RSSI), pilot signal to interference ratio (E_C/I_O), channel, Ethernet status, *etc.* For agents that are in default, the parameter causing the default may be highlighted. For example, if an agent's entry in column 604 is highlighted, as shown at field 615, then the host 102 may not have received a status message from that agent for more than the predetermined time period.

[0026] The screen 600 may also include buttons 625, 627, 629 that allow a user 214 to configure the screen to display various other information. For example selecting Search All button 625 may cause the screen to appear as shown in Figure 6. Selecting the Fault View button 627 may cause the screen to display the default list of agents, for example, as shown in Figure 7. Each row, as shown in Figure 7, may represent an agent 104 that is in default. It will be appreciated that the host 102 may not have received a current status message from an agent 104 in default, and therefore, not all of the fields 616, 618, 620, 622 may be populated for all defaulted agents 104. According to various embodiments, the screen 600 may include a button (not shown) that allows a user 214 to initiate an activity test for a particular agent 104, for example, as described above with respect to step 412.

[0027] The screen 600 may also be configured to display the pending list, as shown in Figure 8, for example, by selecting the button 629. The pending list may include columns and rows similar to Figure 6. Column 650 may list a device identifier for each agent 104 on the pending list. Because agents on the pending list may not have been assigned a device name yet, the identifier shown in column 650 may be an IP address, such as the public IP address shown. Column 611 may show the private IP address for each host. Fields 656 and 658 may respectively show the monthly and daily byte traffic to and from each agent 104. Columns 604 for last status message received and 616, 618, 620, and 622 for agent status information may be blank, as shown in Figure 8. This is because most agents 104 appearing on the pending list have not yet been configured to send the host 102 status messages that would include this information.

[0028] According to various embodiments, agents 104 listed in the screen 600 may be selected and additional data regarding those agents may be displayed, for example, as shown in Figure 9. The additional data may include graphs of historical reports of RSSI (field 670), Ec/Io (field 672), Channel (field 674) and CSMA (field 676). This data may be helpful to the user 214 in determining the status of the displayed agent 104.

[0029] The screen 600 may also include another configuration (not shown) for listing inactive devices. Inactive devices may be devices that are to be taken out of service for business, rather than technical reasons. For example,

when the network 100 is implemented by a bank, inactive devices may include those ATM's that are to be relocated or shut-down.

[0030] According to various embodiments the host 102 may also be configured to perform various statistical analyses of current and historical data received from the agents 104 (*e.g.,* via statistics module 208). The data may have been received from the hosts 104 through current and historical status messages, and may be stored at agent data files. Figure 9A shows a screen 900 for listing various parameters of agents 104. Each row of the screen 900 includes statistical information about a single metric of an agent 104. For example, column 902 lists the name of a relevant agent 104. Column 904 lists the agent metric to be described in a row. Column 906 shows the last value of the metric, (e.g., derived from the last status message received from the agent 104 listed in column 902). Columns 908, 910, 912 and 914 respectively list the mean, mode and median value and standard deviation of the metric over a predetermined time period. A low and high value of the metric for the time period is listed at column 918. A graph 920 of a given metric may be displayed as shown in Figure 9B.

[0031] In addition to, or instead of being made available for review by screen 900, statistical data about agents 104 may be used to monitor agents 104 and troubleshoot potential problems. According to various embodiments, the statistics module 208 may implement dynamic threshold checking on an agent-by-agent basis. It will be appreciated that for different devices, different values of data quantities (*e.g.*, RSSI, Ec/Io, Channel, Ethernet Status, *etc.*) may indicate an agent failure. Accordingly, the statistics module 208 may generate agent-specific failure thresholds for determining when a particular agent 104 or type of agent 104 has failed.

To create agent-specific failure thresholds, historical data from one or more of the agents 104 may be analyzed and distribution properties may be calculated for one or more data quantities. For example, if the distribution of a data quantity over time is normal, then a mean and standard deviation may be found. An agent-specific failure threshold may then be found based on the distribution. For example, if the distribution is normal, the threshold may be exceeded if the current value of the data quantity is more than three standard deviations from the mean value. If the distribution is not normal and/or conforms to a different type of distribution, then other statistical or mathematical techniques as known in the art may be used to develop the thresholds. When an agent 104 meets or exceeds a threshold, it may be added to the default list described above.

[0032] According to various embodiments, the statistics module 208 may also have functionality for predicting agent 104 failures before they occur. For example, upon failure of an agent 104 in the wireless network, current and/or historical data regarding the failed agent 104 (*e.g.,* RSSI, Ec/Io, Channel, Ethernet Status, *etc.*) may be saved as a failure profile. The current and/or historical status data of active agents 104 may then be compared or correlated to the failure profile. Agents 104 having current and/or historical data that correlates highly to the failure profile may be in danger of failure themselves. In various embodiments, failure profiles from multiple failed wireless devices may be aggregated to form master failure profiles. Also, in various embodiments, failure profiles may be categorized based on the type of failure experienced. In this way, specific failure types may be predicted by correlating the data of active devices to a given type of failure profile. The host 102 may handle agents 104 with predicted future failures according to any suitable method. For example, these agents 104 may be added to the default list. According to various embodiments, the agents 104 may be added to a separate list of agents 104 with a high risk of failure.

[0033] According to various embodiments, the host 102 may include additional functionality that may be of use to a user 214. For example, according to various embodiments, the host 102 may include functionality for pushing common configuration parameters to pending agents 104 (*e.g.*, agents 104 that are communicating on the network but have not yet been configured to send periodic status messages). Implementing push to production functionality may cause common configuration parameters to be sent to all pending agents 104, which may advance or complete their configuration. In various embodiments, a user 214 may implement push to production functionality by activating a button on the "Pending" view of screen 600 shown above. After receiving the common configuration parameters, the agents 104 may begin sending periodic status messages. In various embodiments, when the first status message is received from an agent 104, it may be automatically removed from the pending list, for example, according to process flows 400 and 500 above.

[0034] Also, the host 102 may be configured to capture the current system logs (syslog) of one or more agents 104. The syslog of an agent may indicate historical data regarding the agent 104 and/or more detailed information regarding the agent's status. Also, the host 102 may include functionality to allow an operator to manage firmware on the agents 104. For example, the operator may upgrade the firmware on one or more agents 104 (*e.g,* for modems 302, associated devices 304, *etc.*) track firmware versions, track firmware performance, *etc.*

[0035] The host 102 may additionally include functionality for pushing parameters to individual agents 104. For example, instead of pushing common configuration parameters, as described above with respect to the push to production functionality, the user 214 may select any available parameter and push it to one, several or all agents 104, for example, concurrently. This may allow the user 214 to configure one or a few pending agents 104 individually.

[0036] The systems and methods described above may be used to manage new agents 104 being brought onto the network 100. Figure 10 shows a process flow

1000 for bringing an agent 104 onto the network 100. At step 1002, an indication of a new pending agent 104 may be received. For example, the new pending agent 104 may be listed in the pending agent list described above. The new pending agent 104 may appear on the pending agent list for a variety of reasons. For example, the new pending agent 104 may be a newly installed ATM, kiosk or other device that is ready to be activated on the network 100. Also, the modem 302 of an agent 104 or the complete agent 104 may be tested before assembly and/or installation. During this testing, the modem 302 or agent 104 may appear on the network 100 and consequently on the pending agent list as a new agent 104. Accordingly, not all new pending agents 104 are ready to be finally configured.

[0037] Referring back to the process flow 1000, at step 1004, it may be determined whether a new pending agent 104 is ready to be configured by comparing the new pending agent 104 to implementation data. The implementation data may include a list of agents and a target date for when they will be activated on the network 100. The activation date of an agent may be driven by business considerations (*e.g.*, when a new ATM or kiosk is required, how soon it can be assembled and placed, *etc.*). If, at decision step 1006, the new pending agent 104 has appeared on the pending agent list near its scheduled activation date (*e.g.*, within a few days), then the new pending agent 104 may be configured to send periodic status messages at step 1010. If the new pending agent 104 has appeared on the pending agent list at a time not near its scheduled activation time, this may indicate that the new pending agent 104 is only being tested or is not otherwise ready to be configured on the network 100. In that case, its appearance may be recorded at step 1008. According to various embodiments, the pending agent 104 may then be deleted from the pending agent list.

[0038] It is to be understood that the figures and descriptions of the present invention have been simplified to illustrate elements that are relevant for a clear understanding of the present invention, while eliminating other elements, for purposes of clarity. Those of ordinary skill in the art will recognize that these and other elements may be desirable. However, because such elements are well known in the art and because they do not facilitate a better understanding of the present invention, a discussion of such elements is not provided herein.

[0039] As used herein, a "computer," "computer system," and the like, may be, for example and without limitation, either alone or in combination, a personal computer (PC), server-based computer, main frame, server, microcomputer, minicomputer, laptop, personal data assistant (PDA), cellular phone, pager, processor, including wireless and/or wireline varieties thereof, a virtual computer system and/or any other computerized device or construct capable of configuration for processing data for standalone application and/or over a networked medium or media. Computers and computer systems disclosed herein may include operatively associated memory for storing certain software applications used in obtaining, processing, storing and/or communicating data. It can be appreciated that such memory can be internal, external, remote or local with respect to its operatively associated computer or computer system. Memory may also include any means for storing software or other instructions including, for example and without limitation, a hard disk, an optical disk, floppy disk, ROM (read only memory), RAM (random access memory), PROM (programmable ROM), EEPROM (extended erasable PROM), and/or other like computer-readable media.

[0040] The described systems may include various modules and/or components implemented as software code to be executed by a processor(s) of the systems or any other computer system using any type of suitable computer instruction type. The software code may be stored as a series of instructions or commands on a computer readable medium. The term "computer-readable medium" as used herein may include, for example, magnetic and optical memory devices such as diskettes, compact discs of both read-only and writeable varieties, optical disk drives, and hard disk drives. A computer-readable medium may also include memory storage that can be physical, virtual, permanent, temporary, semi-permanent and/or semi-temporary. A computer-readable medium may further include one or more data signals transmitted on one or more carrier waves.

[0041] While several embodiments of the invention have been described, it should be apparent that various modifications, alterations and adaptations to those embodiments may occur to persons skilled in the art with the attainment of some or all of the advantages of the present invention. It is therefore intended to cover all such modifications, alterations and adaptations without departing from the scope of the present invention as defined by the appended claims.

Claims

1. A method of managing a network (100) comprising a plurality of agents (104), the method comprising:

   receiving (402), by a passive module (202) of a host computer (102) in communication with a router (116) and the plurality of agents via the network (100), an unsolicited periodic status message from each of a first group of agents selected from the plurality of agents (104), wherein the host computer (102) includes the passive module (202), an active module (204), a cryptographic module (208), and a statistics module (208);

   querying, by the cryptographic module (206), the router on a local portion (106) of the network (100) positioned to handle communications between components on the local portion (106) of the network and components on a remote por-

tion (108, 110) of the network (100);
receiving, by at least one of the passive (202), active (204), and cryptographic modules (206), from the router (116) an indication of a second group of agents from the plurality of agents (104) that are communicating through the router (116);
comparing, by at least one of the passive (202) and cryptographic (206) modules, the first group of agents to the second group of agents;
generating, by a user interface (212) of the host computer (102), a list of agents communicating through the router (116) from which periodic status messages are not being received; and
implementing, by the statistics module (208), at least one of dynamic threshold checking and predictive agent failure of an agent (104).

2. The method of claim 1, wherein generating the list of agents communicating through the router (116) from which periodic status messages are not being received comprises identifying agents included in the second group of agents and not the first group of agents.

3. The method of claim 1, wherein the second group of agents comprises agents that are passing encrypted communications through the router (116).

4. The method of claim 1, wherein the indication of the second group of agents comprises, for each agent, a private internet protocol (IP) address and a public IP address.

5. The method of claim 4, wherein identifying agents communicating through the router (116) from whom periodic status messages are not being received comprises matching at least one of the private IP address and the public IP address to an agent name.

6. The method of claim 1, further comprising:

storing a plurality of agent data files, wherein each of the agent data files corresponds to a first group of agents selected from the plurality of agents;
upon receiving (402) a status message from a first agent, updating (404) an agent data file corresponding to the first agent;
periodically identifying (406) agent data files from the plurality of agent data files that have not been updated for a predetermined amount of time; and
sending (410) a request for response to a second agent corresponding to an agent data file that has not been updated for a predetermined amount of time.

7. The method of claim 1, further comprising compiling a list of pending agents communicating through the router (116) from whom periodic status messages are not being received.

8. The method of claim 1, further comprising pushing configuration profiles to the agents communicating through the router (116) from whom periodic status messages are not being received, wherein the configuration profiles configure the agents to send periodic status messages.

9. A computer system comprising:

a plurality of agents (104), each agent including an associated device (304), an agent data store (306), and a modem (302);
a router (116) positioned on a local portion (106) of a network (100) and positioned to handle communications between components on the local portion (106) of the network and components on a remote portion (108, 110) of the network; and
a host computer (102) including a passive module (202), an active module (204), a cryptographic module (206), and a statistics module (208) in communication with the plurality of agents (104) and the router (116) via the network (100), wherein the host computer (102) is configured to:

receive (402), by the passive module (202), an unsolicited periodic status message from each of a first group of agents selected from the plurality of agents;
query, by the cryptographic module (206), the router (116) for an indication of a second group of agents (104) from the plurality of agents that are communicating through the router (116);
receive, by at least one of the passive (202), active (204), and cryptographic (206) modules, from the router (116) the indication of the second group of agents from the plurality of agents that are communicating through the router (116);
compare, by at least one of the passive (202) and cryptographic modules (206), the first group of agents to the second group of agents;
generate, by a user interface (212) of the host computer (102), a list of agents communicating through the router (116) from which periodic status messages are not being received; and
implement, by the statistics module (208), at least one of dynamic threshold checking and predictive agent failure of an agent.

10. The computer system of claim 9, wherein the host computer (102) is further configured to generate the list of agents communicating through the router (116) from which periodic status messages are not being received by identifying agents included in the second group of agents and not the first group of agents.

11. The computer system of claim 9, wherein the second group of agents comprises agents that are passing encrypted communications through the router (116).

12. The computer system of claim 9, wherein the indication of the second group of agents comprises, for each agent, a private internet protocol (IP) address and a public IP address.

13. The computer system of claim 12, wherein identifying agents communicating through the router (116) from whom periodic status messages are not being received comprises matching at least one of the private IP address and the public IP address to an agent name.

14. The computer system of claim 9, wherein the host computer (102) is further configured to:

store a plurality of agent data files, wherein each of the agent data files corresponds to a first group of agents selected from the plurality of agents;
upon receiving (402) a status message from a first agent, update (404) an agent data file corresponding to the first agent;
periodically identify (406) agent data files from the plurality of agent data files that have not been updated for a predetermined amount of time; and
send (410) a request for response to a second agent corresponding to an agent data file that has not been updated for a predetermined amount of time.

15. The computer system of claim 9, wherein the host computer (102) is further configured to compile a list of pending agents communicating through the router (116) from whom periodic status messages are not being received.

16. The computer system of claim 9, further comprising pushing configuration profiles to the agents communicating through the router (116) from whom periodic status messages are not being received, wherein the configuration profiles configure the agents to send periodic status messages.

17. A computer readable medium having instructions stored thereon that, when executed by a host computer (102) in communication with a router (116) and a plurality of agents (104) via a network (100), cause the host computer (102) to perform the method steps of any one of claims 1 to 6.

Patentansprüche

1. Verfahren zum Managen eines Netzwerks (100), das eine Vielzahl von Agenten (104) umfasst, wobei das Verfahren umfasst:

Empfangen (402), durch ein passives Modul (202) eines Hostcomputers (102) in Kommunikation mit einem Router (116) und der Vielzahl von Agenten über das Netzwerk (100), einer unverlangten periodischen Zustandsmeldung von jedem einer ersten Gruppe von Agenten, die aus der Vielzahl von Agenten (104) selektiert wurden, wobei der Hostcomputer (102) das passive Modul (202), ein aktives Modul (204), ein kryptografisches Modul (208) und ein statistisches Modul (208) einschließt;
Abfragen, durch das kryptografische Modul (206), des Routers auf einem lokalen Teil (106) des Netzwerks (100), der positioniert ist, Kommunikationen zwischen Komponenten auf dem lokalen Teil (106) des Netzwerks und Komponenten auf einem fernen Teil (108, 110) des Netzwerks (100) zu handhaben;
Empfangen, durch mindestens eins der passiven (202), aktiven (204) und kryptografischen Module (206), vom Router (116) einer Anzeige einer zweiten Gruppe von Agenten aus der Vielzahl von Agenten (104), die durch den Router (116) kommunizieren;
Vergleichen, durch mindestens eins der passiven (202) und kryptografischen (206) Module, der ersten Gruppe von Agenten mit der zweiten Gruppe von Agenten;
Generieren, durch eine Benutzerschnittstelle (212) des Hostcomputers (102), einer Liste von Agenten, die durch den Router (116) kommunizieren, von denen keine periodischen Zustandsmeldungen empfangen werden; und
Implementieren, durch das statistische Modul (208), mindestens einer dynamischen Schwellenwertprüfung bzw. eines voraussagenden Agentenversagens eines Agenten (104).

2. Verfahren nach Anspruch 1, wobei das Generieren einer Liste von Agenten, die durch den Router (116) kommunizieren, von dem keine periodischen Zustandsmeldungen empfangen werden, das Identifizieren von Agenten umfasst, die in der zweiten Gruppe von Agenten und nicht der ersten Gruppe von Agenten inbegriffen sind.

3. Verfahren nach Anspruch 1, wobei die zweite Grup-

pe von Agenten, Agenten umfasst, die verschlüsselte Kommunikationen durch den Router (116) senden.

4. Verfahren nach Anspruch 1, wobei die Anzeige der zweiten Gruppe von Agenten, für jeden Agenten, eine private Internet-Protokoll-Adresse (IP-) und eine öffentliche IP-Adresse umfasst.

5. Verfahren nach Anspruch 4, wobei das Identifizieren von Agenten, die durch den Router (116) kommunizieren, von dem keine periodischen Zustandsmeldungen empfangen werden, die Passung mindestens der privaten IP-Adresse bzw. der öffentlichen IP-Adresse mit einem Agentennamen umfasst.

6. Verfahren nach Anspruch 1, ferner umfassend:

Speichern einer Vielzahl von Agenten-Datendateien, wobei jede der Agenten-Datendateien einer ersten Gruppe von Agenten entspricht, die aus der Vielzahl von Agenten selektiert wurden;
nach Empfangen (402) einer Zustandsmeldung von einem ersten Agenten, Aktualisieren (404) einer Agenten-Datendatei, die dem ersten Agenten entspricht;
periodisches Identifizieren (406) von Agenten-Datendateien aus der Vielzahl von Datendateien, die für eine vorbestimmte Dauer nicht aktualisiert worden sind; und
Senden (410) einer Anforderung für eine Antwort an einen zweiten Agenten, der einer Agenten-Datendatei entspricht, die für eine vorbestimmte Dauer nicht aktualisiert worden ist.

7. Verfahren nach Anspruch 1, das ferner die Erstellung einer Liste von anstehenden Agenten, die durch den Router (116) kommunizieren, von denen keine periodischen Zustandsmeldungen erhalten werden.

8. Verfahren nach Anspruch 1, das ferner das Puschen von Konfigurationsprofilen zu Agenten umfasst, die durch den Router (116) kommunizieren, von dem keine periodischen Zustandsmeldungen empfangen werden, wobei die Konfigurationsprofile die Agenten konfigurieren, periodischen Zustandsmeldungen zu senden.

9. Computersystem, umfassend:

Eine Vielzahl von Agenten (104), wobei jeder Agent ein zugehöriges Gerät (304), einen Agentendatenspeicher (306) und ein Modem (302) einschließt;
einen Router (116), der auf einem lokalen Teil (106) des Netzwerks (100) positioniert ist und positioniert ist, Kommunikationen zwischen Komponenten auf dem lokalen Teil (106) des Netzwerks und Komponenten auf einem fernen Teil (108, 110) des Netzwerks zu handhaben; und
einen Hostcomputer (102), der ein passives Modul (202), ein aktives Modul (204), ein kryptografisches Modul (206) und ein statistisches Modul (208) in Kommunikation mit der Vielzahl von Agenten (104) und dem Router (116) über das Netzwerk (100) einschließt, wobei der Hostcomputer (102) konfiguriert ist, Folgendes zu tun:

Empfangen (402), durch das passive Modul (202), einer unverlangten periodischen Zustandsmeldung von jedem einer ersten Gruppe von Agenten, die aus der Vielzahl von Agenten selektiert wurden;
Abfragen, durch das kryptografische Modul (206), des Routers (116) nach einer Anzeige einer zweiten Gruppe von Agenten (104) aus der Vielzahl von Agenten, die durch den Router (116) kommunizieren;
Empfangen, durch mindestens eins der passiven (202), aktiven (204) und kryptografischen Module (206), vom Router (116) der Anzeige der zweiten Gruppe von Agenten aus der Vielzahl von Agenten, die durch den Router (116) kommunizieren;
Vergleichen, durch mindestens eins der passiven (202) und kryptografischen (206) Module, der ersten Gruppe von Agenten mit der zweiten Gruppe von Agenten;
Generieren, durch eine Benutzerschnittstelle (212) des Hostcomputers (102), einer Liste von Agenten, die durch den Router (116) kommunizieren, von denen keine periodischen Zustandsmeldungen empfangen werden; und
Implementieren, durch das statistische Modul (208), mindestens einer dynamischen Schwellenwertprüfung bzw. eines voraussagenden Agentenversagens eines Agenten .

10. Computersystem nach Anspruch 9, wobei der Hostcomputer (102) ferner konfiguriert ist, eine Liste von Agenten, die durch den Router (116) kommunizieren, von dem keine periodischen Zustandsmeldungen empfangen werden, durch das Identifizieren von Agenten zu generieren, die in der zweiten Gruppe von Agenten und nicht der ersten Gruppe von Agenten inbegriffen sind.

11. Computersystem nach Anspruch 9, wobei die zweite Gruppe von Agenten, Agenten umfasst, die verschlüsselte Kommunikationen durch den Router (116) senden.

12. Computersystem nach Anspruch 9, wobei die An-

zeige der zweiten Gruppe von Agenten, für jeden Agenten, eine private Internet-Protokoll-Adresse (IP-) und eine öffentliche IP-Adresse umfasst.

13. Computersystem nach Anspruch 12, wobei das Identifizieren von Agenten, die durch den Router (116) kommunizieren, von dem keine periodischen Zustandsmeldungen empfangen werden, die Passung mindestens der privaten IP-Adresse bzw. der öffentlichen IP-Adresse mit einem Agentennamen umfasst.

14. Computersystem nach Anspruch 9, wobei der Hostcomputer (102) ferner konfiguriert ist, Folgendes zu tun:

Speichern einer Vielzahl von Agenten-Datendateien, wobei jede der Agenten-Datendateien einer ersten Gruppe von Agenten entspricht, die aus der Vielzahl von Agenten selektiert wurden;
nach Empfangen (402) einer Zustandsmeldung von einem ersten Agenten, Aktualisieren (404) einer Agenten-Datendatei, die dem ersten Agenten entspricht;
periodisches Identifizieren (406) von Agenten-Datendateien aus der Vielzahl von Datendateien, die für eine vorbestimmte Dauer nicht aktualisiert worden sind; und
Senden (410) einer Anforderung für eine Antwort an einen zweiten Agenten, der einer Agenten-Datendatei entspricht, die für eine vorbestimmte Dauer nicht aktualisiert worden ist.

15. Computersystem nach Anspruch 9, wobei der Hostcomputer (102) das ferner konfiguriert ist, eine Liste von anstehenden Agenten zu erstellen, die durch den Router (116) kommunizieren, von denen keine periodischen Zustandsmeldungen erhalten werden.

16. Computersystem nach Anspruch 9, das ferner das Puschen von Konfigurationsprofilen zu Agenten umfasst, die durch den Router (116) kommunizieren, von dem keine periodischen Zustandsmeldungen empfangen werden, wobei die Konfigurationsprofile die Agenten konfigurieren, periodischen Zustandsmeldungen zu senden.

17. Computerlesbares Medium mit darauf gespeicherten Befehlen, die, wenn von einem Hostcomputer (102) in Kommunikation mit einem Router (116) und einer Vielzahl von Agenten (104) über ein Netzwerk (100) ausgeführt, bewirken, dass der Hostcomputer (102) die Verfahrensschritte nach einem der Ansprüche 1 bis 6 durchführt.

Revendications

1. Procédé de gestion d'un réseau (100) comportant une pluralité d'agents (104), le procédé comportant :

la réception (402), par un module passif (202) d'un ordinateur hôte (102) en communication avec un routeur (116) et la pluralité d'agents par l'intermédiaire du réseau (100), d'un message d'état périodique non sollicité de chacun d'un premier groupe d'agents sélectionnés parmi la pluralité d'agents (104), dans lequel l'ordinateur hôte (102) comprend le module passif (202), un module actif (204), un module cryptographique (208), et un module statistique (208) ;
l'interrogation, par le module cryptographique (206), du routeur sur une partie locale (106) du réseau (100) positionné pour gérer les communications entre les composants sur la partie locale (106) du réseau et les composants sur une partie éloignée (108, 110) du réseau (100) ;
la réception, par au moins le module passif (202), actif (204), et/ou cryptographique (206), en provenance du routeur (116), d'une indication d'un second groupe d'agents parmi la pluralité d'agents (104) qui communiquent à travers le routeur (116) ;
la comparaison, par au moins le module passif (202) et/ou cryptographique (206), du premier groupe d'agents avec le second groupe d'agents ;
la production, par une interface utilisateur (212) de l'ordinateur hôte (102), d'une liste d'agents communiquant à travers le routeur (116) d'où des messages d'état périodiques ne sont pas reçus ; et
la mise en oeuvre, par le module statistique (208), d'au moins une vérification de seuil dynamique et/ou un échec d'agent prédictif (104) d'un agent.

2. Procédé selon la revendication 1, dans lequel la production de la liste d'agents communiquant à travers le routeur (116) d'où des messages d'état périodiques ne sont pas reçus comporte l'identification d'agents compris dans le second groupe d'agents et non dans le premier groupe d'agents.

3. Procédé selon la revendication 1, dans lequel le second groupe d'agents comporte des agents qui font passer des communications chiffrées à travers le routeur (116).

4. Procédé selon la revendication 1, dans lequel l'indication que le second groupe d'agents comporte, pour chaque agent, une adresse de protocole Internet (IP) privée et une adresse IP publique.

5. Procédé selon la revendication 4, dans lequel l'identification d'agents communiquant à travers le routeur (116) d'où des messages d'état périodiques ne sont pas reçus comporte la mise en correspondance d'au moins l'adresse IP privée et/ou l'adresse IP publique avec un nom d'agent.

6. Procédé selon la revendication 1, comportant en outre :

la mémorisation d'une pluralité de fichiers de données d'agent, dans lequel chacun des fichiers de données d'agent correspond à un premier groupe d'agents sélectionnés parmi la pluralité d'agents ;
au moment de la réception (402) d'un message d'état en provenance d'un premier agent, la mise à jour (404) d'un fichier de données d'agent correspondant au premier agent ;
l'identification périodique (406) de fichiers de données d'agent parmi la pluralité de fichiers de données d'agent qui n'ont pas été mis à jour depuis une période de temps prédéterminée ; et
l'envoi (410) d'une demande de réponse à un second agent correspondant à un fichier de données d'agent qui n'a pas été mis à jour depuis une période de temps prédéterminée.

7. Procédé selon la revendication 1, comportant en outre la compilation d'une liste d'agents en attente communiquant à travers le routeur (116) d'où des messages d'état périodiques ne sont pas reçus.

8. Procédé selon la revendication 1, comportant en outre la poussée de profils de configuration vers les agents communiquant à travers le routeur (116) d'où des messages d'état périodiques ne sont pas reçus, dans lequel les profils de configuration configurent les agents pour qu'ils envoient des messages d'état périodiques.

9. Système d'ordinateur comportant :

une pluralité d'agents (104), chaque agent comprenant un dispositif associé (304), une mémoire de données d'agent (306), et un modem (302) ;
un routeur (116) positionné sur une partie locale (106) d'un réseau (100) et positionné pour gérer les communications entre des composants sur la partie locale (106) du réseau et des composants sur une partie éloignée (108, 110) du réseau ; et
un ordinateur hôte (102) comprenant un module passif (202), un module actif (204), un module cryptographique (206), et un module statistique (208) en communication avec la pluralité d'agents (104) et le routeur (116) par l'intermédiaire du réseau (100), dans lequel l'ordinateur hôte (102) est configuré pour :

recevoir (402), par le module passif (202), un message d'état périodique non sollicité en provenance de chacun d'un premier groupe d'agents sélectionnés parmi la pluralité d'agents ;
interroger, par le module cryptographique (206), le routeur (116) pour une indication d'un second groupe d'agents (104) parmi la pluralité d'agents qui communiquent à travers le routeur (116) ;
recevoir, par au moins le module passif (202), actif (204), et/ou cryptographique (206), en provenance du routeur (116) l'indication du second groupe d'agents parmi la pluralité d'agents qui communiquent à travers le routeur (116) ;
comparer, par au moins le module passif (202) et/ou cryptographique (206) le premier groupe d'agents avec le second groupe d'agents ;
produire, par une interface utilisateur (212) de l'ordinateur hôte (102), une liste d'agents communiquant à travers le routeur (116) d'où des messages d'état périodiques ne sont pas reçus ; et
mettre en oeuvre, par le module statistique (208), d'au moins une vérification de seuil dynamique et/ou un échec d'agent prédictif d'un agent.

10. Système d'ordinateur selon la revendication 9, dans lequel l'ordinateur hôte (102) est en outre configuré pour produire la liste d'agents communiquant à travers le routeur (116) d'où des messages d'état périodiques ne sont pas reçus par les agents d'identification compris dans le second groupe d'agents et non le premier groupe d'agents.

11. Système d'ordinateur selon la revendication 9, dans lequel le second groupe d'agents comporte des agents qui font passer des communications chiffrées à travers le routeur (116).

12. Système d'ordinateur selon la revendication 9, dans lequel l'indication du second groupe d'agents comporte, pour chaque agent, une adresse de protocole Internet (IP) privée et une adresse IP publique.

13. Système d'ordinateur selon la revendication 12, dans lequel l'identification d'agents communiquant à travers le routeur (116) d'où des messages d'état périodiques ne sont pas reçus comporte la mise en correspondance d'au moins l'adresse IP privée et/ou l'adresse IP publique avec un nom d'agent.

14. Système d'ordinateur selon la revendication 9, dans lequel l'ordinateur hôte (102) est en outre configuré pour :

mémoriser une pluralité de fichiers de données d'agent, chacun des fichiers de données d'agent correspondant à premier groupe d'agents sélectionnés parmi la pluralité d'agents ;
au moment de la réception (402) d'un message d'état en provenance d'un premier agent, mettre à jour (404) un fichier de données d'agent correspondant au premier agent ;
identifier périodiquement (406) des fichiers de données d'agent parmi la pluralité de fichiers de données d'agent qui n'ont pas été mis à jour depuis une période de temps prédéterminée ; et
envoyer (410) une demande de réponse à un second agent correspondant à un fichier de données d'agent qui n'a pas été mis à jour depuis une période de temps prédéterminée.

15. Système d'ordinateur selon la revendication 9, dans lequel l'ordinateur hôte (102) est en outre configuré pour compiler une liste d'agents en attente communiquant à travers le routeur (116) d'où des messages d'état périodiques ne sont pas reçus.

16. Système d'ordinateur selon la revendication 9, comportant en outre la poussée de profils de configuration vers les agents communiquant à travers le routeur (116) d'où des messages d'état périodiques ne sont pas reçus, dans lequel les profils de configuration configurent les agents pour qu'ils envoient des messages d'état périodiques.

17. Support lisible par ordinateur ayant des instructions mémorisées à l'intérieur de celui-ci qui, lorsque celles-ci sont exécutées par un ordinateur hôte (102) en communication avec un routeur (116) et une pluralité d'agents (104) par l'intermédiaire d'un réseau (100), amènent l'ordinateur hôte (102) à effectuer les étapes du procédé selon l'une quelconque des revendications 1 à 6.

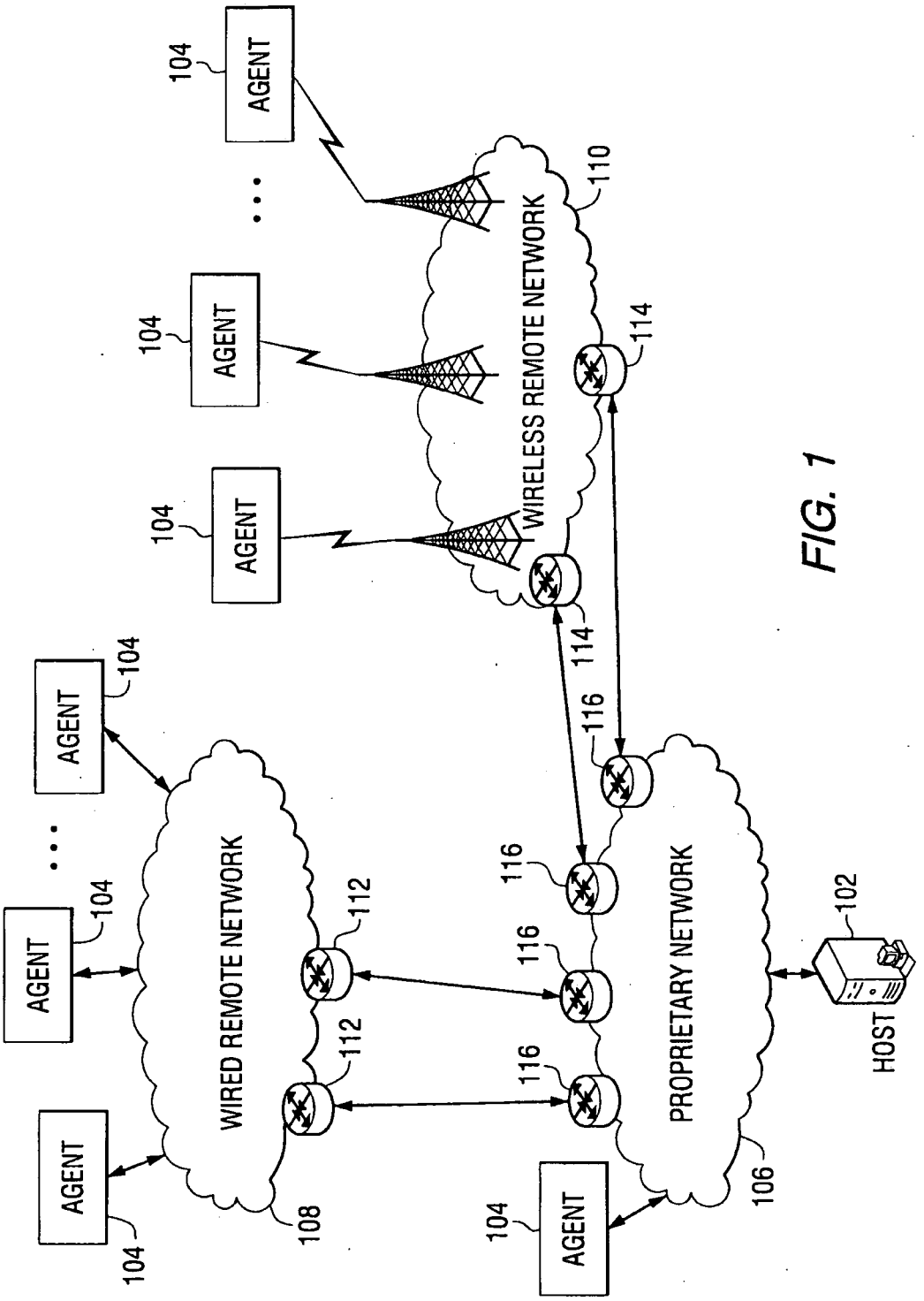

AGENT
104
WIRELESS REMOTE NETWORK
110
114
116
WIRED REMOTE NETWORK
108
112
PROPRIETARY NETWORK
106
102
HOST

FIG. 1

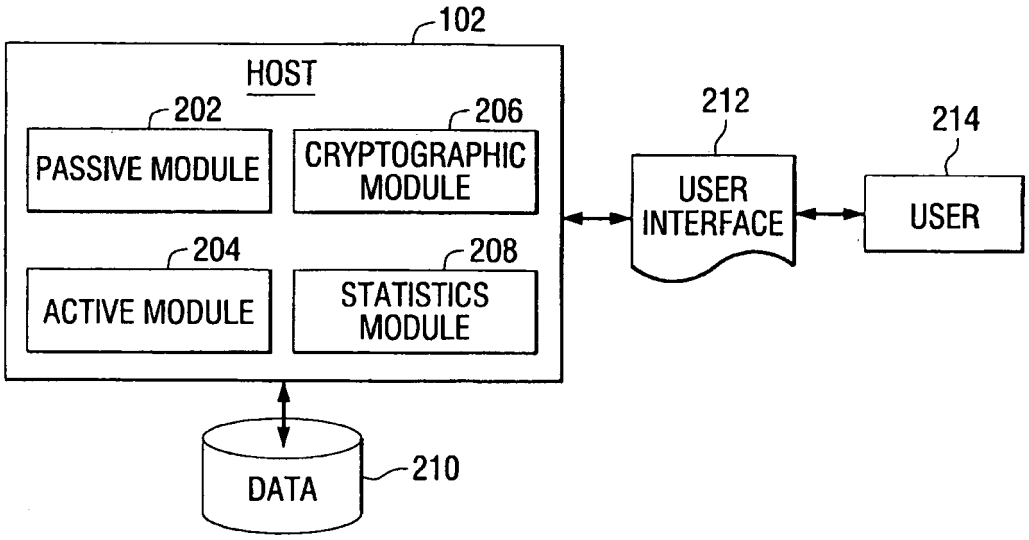

102
HOST
202
PASSIVE MODULE
206
CRYPTOGRAPHIC MODULE
204
ACTIVE MODULE
208
STATISTICS MODULE
212
USER INTERFACE
214
USER
DATA
210

FIG. 2

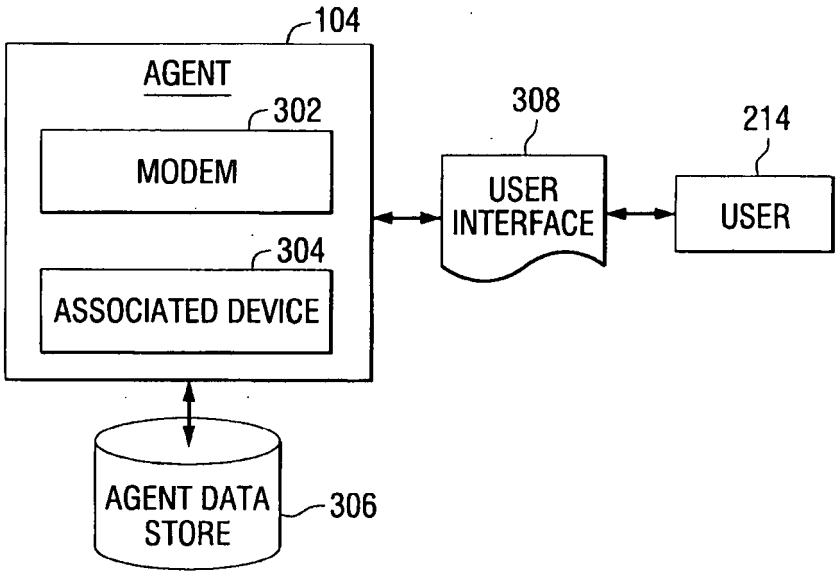

104
AGENT
302
MODEM
304
ASSOCIATED DEVICE
308
USER INTERFACE
214
USER
AGENT DATA STORE
306

FIG. 3

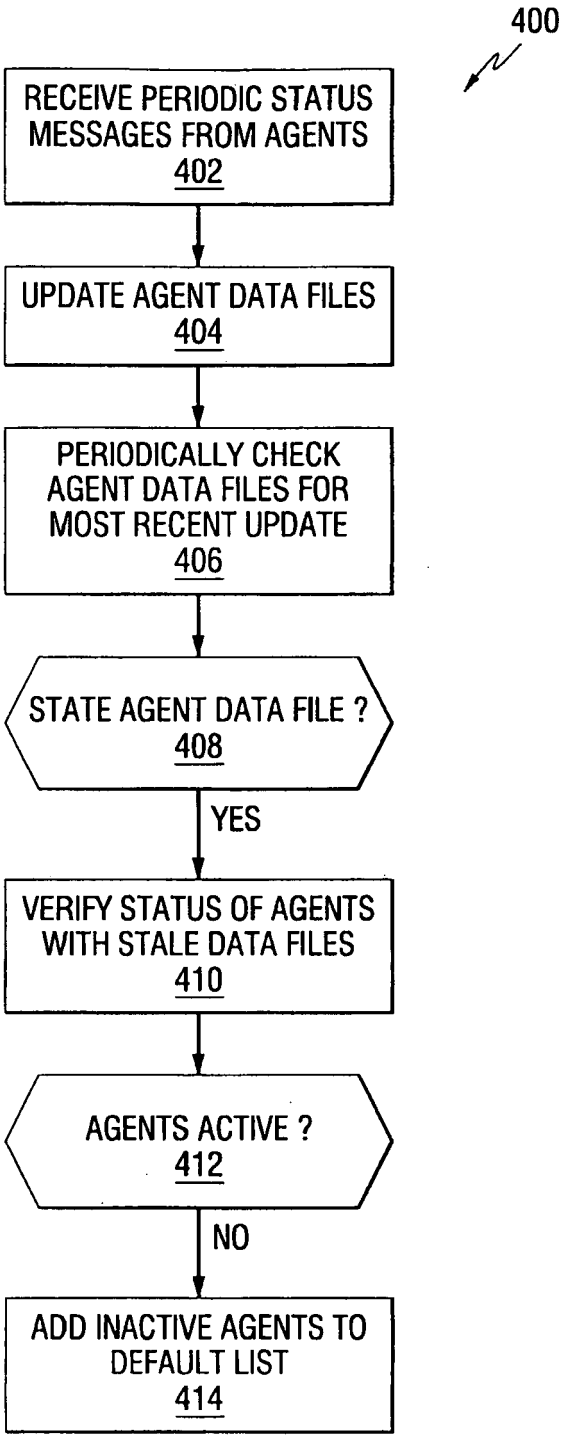

400
RECEIVE PERIODIC STATUS MESSAGES FROM AGENTS
402
UPDATE AGENT DATA FILES
404
PERIODICALLY CHECK AGENT DATA FILES FOR MOST RECENT UPDATE
406
STATE AGENT DATA FILE ?
408
YES
VERIFY STATUS OF AGENTS WITH STALE DATA FILES
410
AGENTS ACTIVE ?
412
NO
ADD INACTIVE AGENTS TO DEFAULT LIST
414

FIG. 4

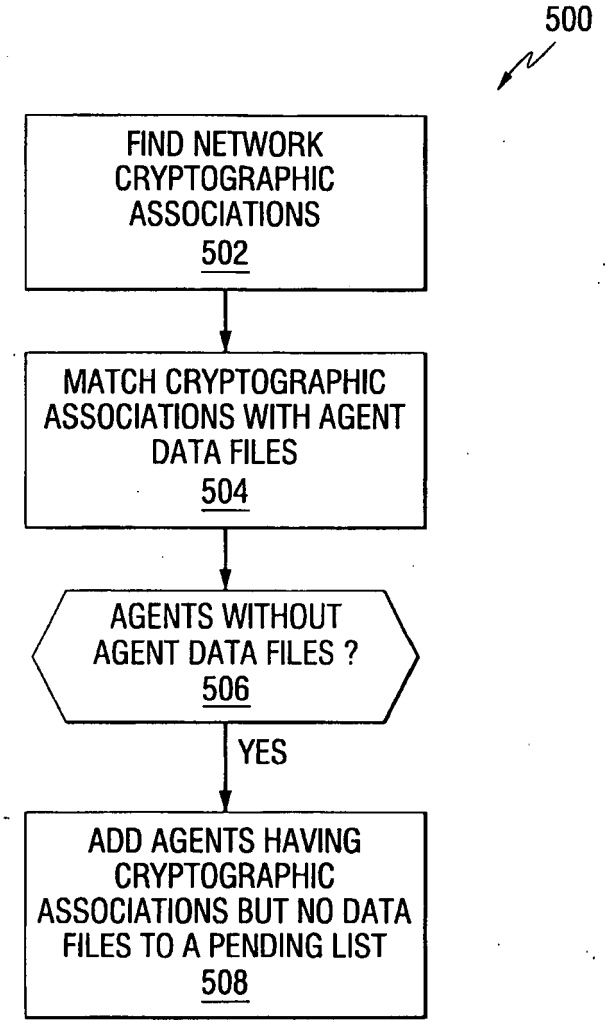

500
FIND NETWORK CRYPTOGRAPHIC ASSOCIATIONS
502
MATCH CRYPTOGRAPHIC ASSOCIATIONS WITH AGENT DATA FILES
504
AGENTS WITHOUT AGENT DATA FILES ?
506
YES
ADD AGENTS HAVING CRYPTOGRAPHIC ASSOCIATIONS BUT NO DATA FILES TO A PENDING LIST
508

FIG. 5

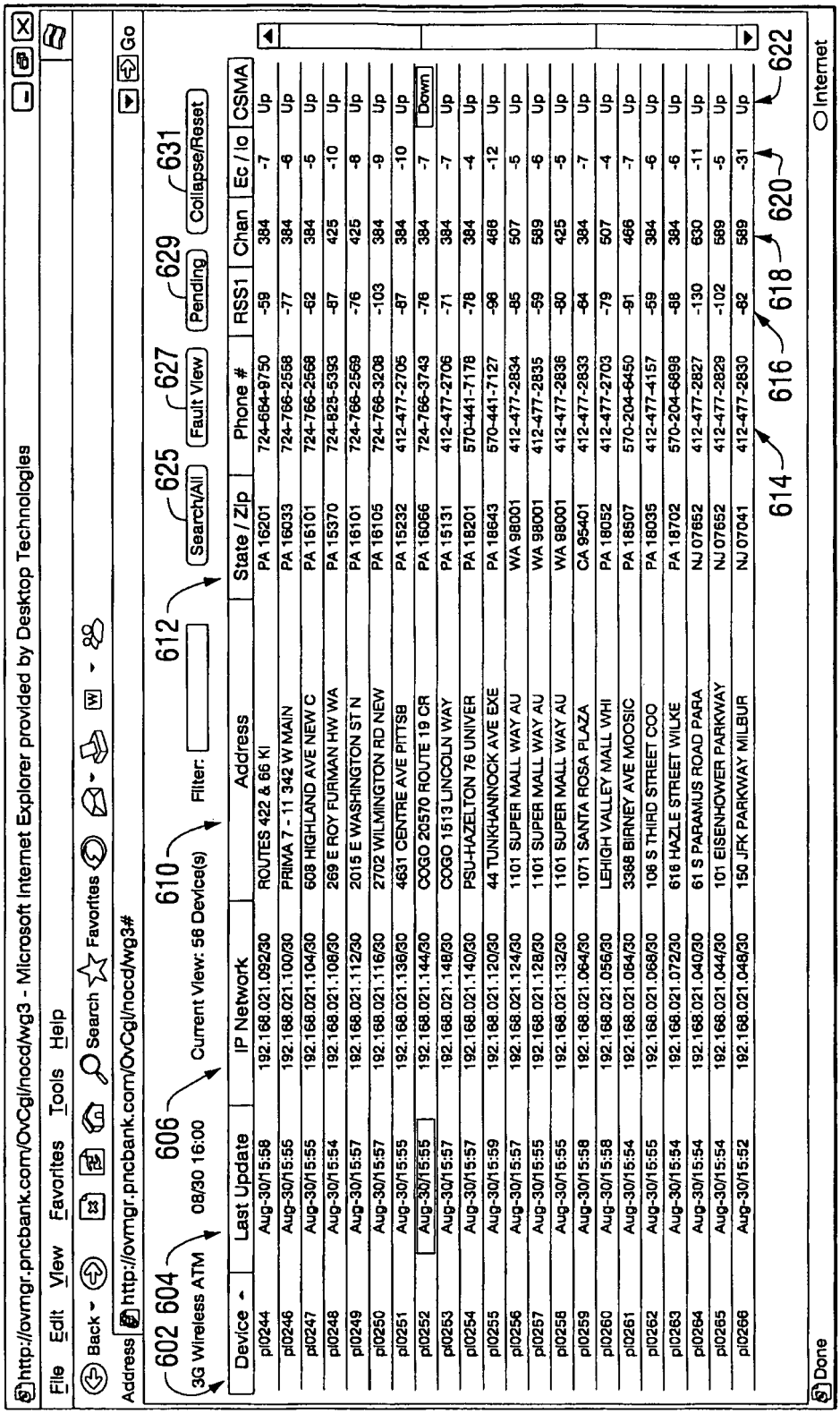

http://ovmgr.pncbank.com/OvCgi/nocd/wg3 - Microsoft Internet Explorer provided by Desktop Technologies
File Edit View Favorites Tools Help
Back Search Favorites
Address http://ovmgr.pncbank.com/OvCgi/nocd/wg3#
Go
602
604
606
610
612
625
627
629
631
3G Wireless ATM
08/30 16:00
Current View: 58 Device(s)
Filter:
Search/All
Fault View
Pending
Collapse/Reset
Device
Last Update
IP Network
Address
State / Zip
Phone #
RSS1
Chan
Ec / Io
CSMA
pl0244 Aug-30/15:58 192.168.021.092/30 ROUTES 422 & 66 KI PA 16201 724-664-9750 -59 384 -7 Up
pl0246 Aug-30/15:55 192.168.021.100/30 PRIMA 7 - 11 342 W MAIN PA 16033 724-766-2568 -77 384 -8 Up
pl0247 Aug-30/15:55 192.168.021.104/30 608 HIGHLAND AVE NEW C PA 16101 724-766-2568 -62 384 -5 Up
pl0248 Aug-30/15:54 192.168.021.108/30 269 E ROY FURMAN HW WA PA 15370 724-825-5393 -87 425 -10 Up
pl0249 Aug-30/15:57 192.168.021.112/30 2015 E WASHINGTON ST N PA 16101 724-766-2569 -76 425 -8 Up
pl0250 Aug-30/15:57 192.168.021.116/30 2702 WILMINGTON RD NEW PA 16105 724-766-3208 -103 384 -9 Up
pl0251 Aug-30/15:55 192.168.021.136/30 4631 CENTRE AVE PITTSB PA 15232 412-477-2705 -87 384 -10 Up
pl0252 Aug-30/15:55 192.168.021.144/30 COGO 20570 ROUTE 19 CR PA 16066 724-766-3743 -76 384 -7 Down
pl0253 Aug-30/15:57 192.168.021.148/30 COGO 1513 LINCOLN WAY PA 15131 412-477-2706 -71 384 -7 Up
pl0254 Aug-30/15:57 192.168.021.140/30 PSU-HAZELTON 76 UNIVER PA 18201 570-441-7178 -78 384 -4 Up
pl0255 Aug-30/15:59 192.168.021.120/30 44 TUNKHANNOCK AVE EXE PA 18643 570-441-7127 -96 468 -12 Up
pl0256 Aug-30/15:57 192.168.021.124/30 1101 SUPER MALL WAY AU WA 98001 412-477-2834 -85 507 -5 Up
pl0257 Aug-30/15:55 192.168.021.128/30 1101 SUPER MALL WAY AU WA 98001 412-477-2835 -59 589 -6 Up
pl0258 Aug-30/15:55 192.168.021.132/30 1101 SUPER MALL WAY AU WA 98001 412-477-2836 -80 425 -5 Up
pl0259 Aug-30/15:58 192.168.021.064/30 1071 SANTA ROSA PLAZA CA 95401 412-477-2833 -64 384 -7 Up
pl0260 Aug-30/15:58 192.168.021.056/30 LEHIGH VALLEY MALL WHI PA 18052 412-477-2703 -79 507 -4 Up
pl0261 Aug-30/15:54 192.168.021.064/30 3368 BIRNEY AVE MOOSIC PA 18507 570-204-6450 -91 468 -7 Up
pl0262 Aug-30/15:55 192.168.021.068/30 106 S THIRD STREET COO PA 18035 412-477-4157 -59 384 -6 Up
pl0263 Aug-30/15:54 192.168.021.072/30 616 HAZLE STREET WILKE PA 18702 570-204-6898 -88 384 -6 Up
pl0264 Aug-30/15:54 192.168.021.040/30 61 S PARAMUS ROAD PARA NJ 07652 412-477-2827 -130 630 -11 Up
pl0265 Aug-30/15:54 192.168.021.044/30 101 EISENHOWER PARKWAY NJ 07652 412-477-2829 -102 589 -5 Up
pl0266 Aug-30/15:52 192.168.021.048/30 150 JFK PARKWAY MILBUR NJ 07041 412-477-2830 -82 589 -31 Up
614
616
618
620
622
Done
Internet

FIG. 6

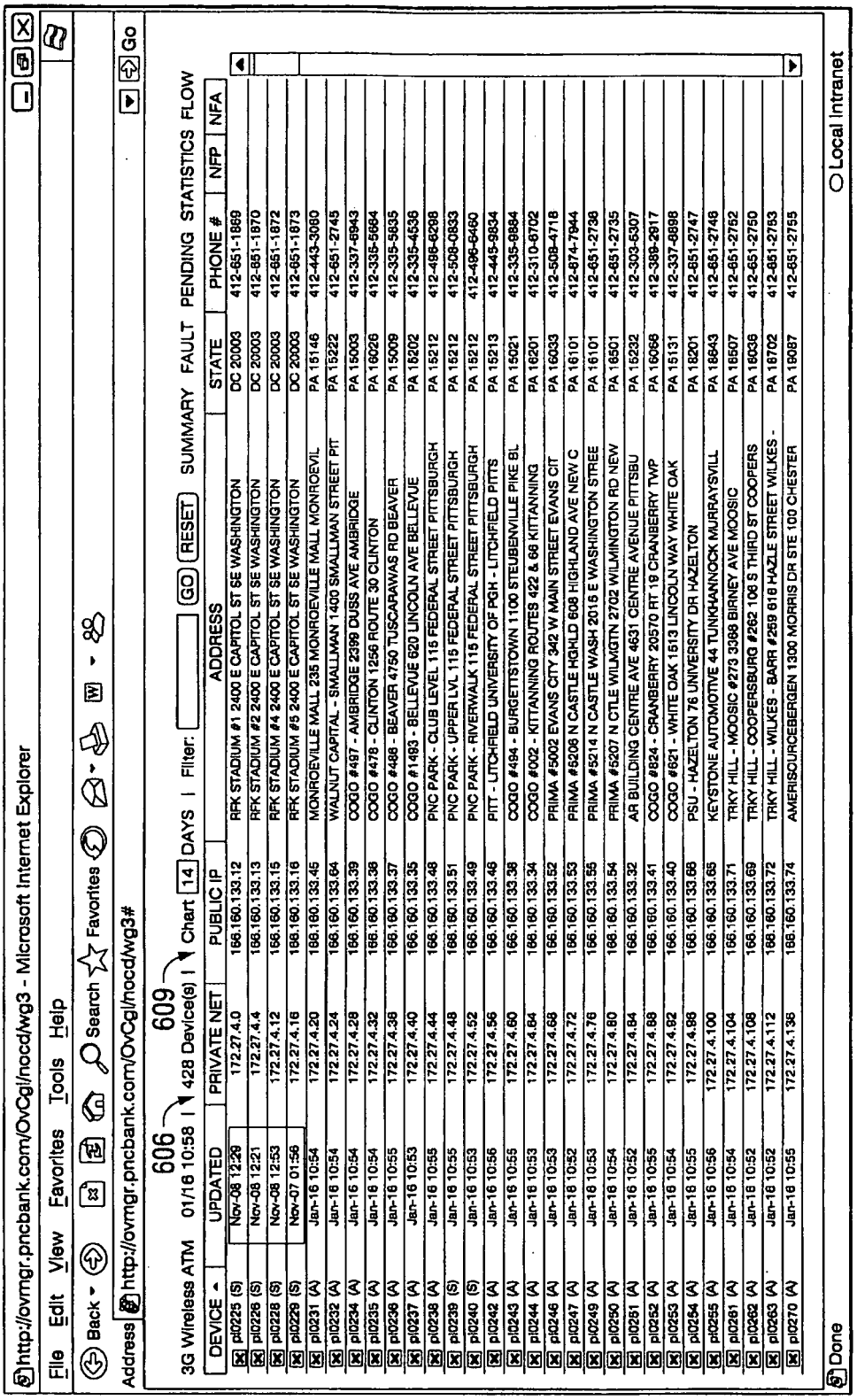

600
http://ovmgr.pncbank.com/OvCgi/nocd/wg3 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://ovmgr.pncbank.com/OvCgi/nocd/wg3#
Go
606
609
3G Wireless ATM 01/16 10:58 | 428 Device(s) | Chart 14 DAYS | Filter: GO RESET SUMMARY FAULT PENDING STATISTICS FLOW
DEVICE UPDATED PRIVATE NET PUBLIC IP ADDRESS STATE PHONE # NFP NFA
pi0225 (S) Nov-06 12:26 172.27.4.0 166.160.133.12 RFK STADIUM #1 2400 E CAPITOL ST SE WASHINGTON DC 20003 412-651-1869
pi0226 (S) Nov-06 12:21 172.27.4.4 166.160.133.13 RFK STADIUM #2 2400 E CAPITOL ST SE WASHINGTON DC 20003 412-651-1870
pi0228 (S) Nov-06 12:53 172.27.4.12 166.160.133.15 RFK STADIUM #4 2400 E CAPITOL ST SE WASHINGTON DC 20003 412-651-1872
pi0229 (S) Nov-07 01:56 172.27.4.16 166.160.133.16 RFK STADIUM #5 2400 E CAPITOL ST SE WASHINGTON DC 20003 412-651-1873
pi0231 (A) Jan-16 10:54 172.27.4.20 166.160.133.45 MONROEVILLE MALL 235 MONROEVILLE MALL MONROEVIL PA 15146 412-443-3060
pi0232 (A) Jan-16 10:54 172.27.4.24 166.160.133.64 WALNUT CAPITAL - SMALLMAN 1400 SMALLMAN STREET PIT PA 15222 412-651-2745
pi0234 (A) Jan-16 10:54 172.27.4.28 166.160.133.39 COGO #497 - AMBRIDGE 2399 DUSS AVE AMBRIDGE PA 15003 412-337-6943
pi0235 (A) Jan-16 10:54 172.27.4.32 166.160.133.38 COGO #478 - CLINTON 1256 ROUTE 30 CLINTON PA 16026 412-335-5684
pi0236 (A) Jan-16 10:55 172.27.4.36 166.160.133.37 COGO #488 - BEAVER 4750 TUSCARAWAS RD BEAVER PA 15009 412-335-5835
pi0237 (A) Jan-16 10:53 172.27.4.40 166.160.133.35 COGO #1493 - BELLEVUE 620 LINCOLN AVE BELLEVUE PA 15202 412-335-4536
pi0238 (A) Jan-16 10:55 172.27.4.44 166.160.133.48 PNC PARK - CLUB LEVEL 115 FEDERAL STREET PITTSBURGH PA 15212 412-496-6298
pi0239 (S) Jan-16 10:55 172.27.4.48 166.160.133.51 PNC PARK - UPPER LVL 115 FEDERAL STREET PITTSBURGH PA 15212 412-508-0833
pi0240 (S) Jan-16 10:53 172.27.4.52 166.160.133.49 PNC PARK - RIVERWALK 115 FEDERAL STREET PITTSBURGH PA 15212 412-496-6460
pi0242 (A) Jan-16 10:56 172.27.4.56 166.160.133.46 PITT - LITCHFIELD UNIVERSITY OF PGH - LITCHFIELD PITTS PA 15213 412-445-9834
pi0243 (A) Jan-16 10:55 172.27.4.60 166.160.133.36 COGO #494 - BURGETTSTOWN 1100 STEUBENVILLE PIKE BL PA 15021 412-335-9884
pi0244 (A) Jan-16 10:53 172.27.4.64 166.160.133.34 COGO #002 - KITTANNING ROUTE9 422 & 66 KITTANNING PA 16201 412-310-6702
pi0246 (A) Jan-16 10:53 172.27.4.68 166.160.133.52 PRIMA #5002 EVANS CITY 342 W MAIN STREET EVANS CIT PA 16033 412-568-4718
pi0247 (A) Jan-16 10:52 172.27.4.72 166.160.133.53 PRIMA #5206 N CASTLE HGHLD 608 HIGHLAND AVE NEW C PA 16101 412-874-7944
pi0249 (A) Jan-16 10:53 172.27.4.76 166.160.133.55 PRIMA #5214 N CASTLE WASH 2015 E WASHINGTON STREE PA 16101 412-651-2738
pi0250 (A) Jan-16 10:54 172.27.4.80 166.160.133.54 PRIMA #5207 N CTLE WILMGTN 2702 WILMINGTON RD NEW PA 16501 412-651-2735
pi0251 (A) Jan-16 10:52 172.27.4.84 166.160.133.32 AR BUILDING CENTRE AVE 4631 CENTRE AVENUE PITTSBU PA 15232 412-303-5307
pi0252 (A) Jan-16 10:55 172.27.4.88 166.160.133.41 COGO #824 - CRANBERRY 20570 RT 19 CRANBERRY TWP PA 16066 412-389-2917
pi0253 (A) Jan-16 10:54 172.27.4.92 166.160.133.40 COGO #821 - WHITE OAK 1513 LINCOLN WAY WHITE OAK PA 15131 412-337-8898
pi0254 (A) Jan-16 10:55 172.27.4.96 166.160.133.66 PSU - HAZELTON 76 UNIVERSITY DR HAZELTON PA 18201 412-651-2747
pi0255 (A) Jan-16 10:56 172.27.4.100 166.160.133.65 KEYSTONE AUTOMOTIVE 44 TUNKHANNOCK MURRAYSVILL PA 18643 412-651-2746
pi0261 (A) Jan-16 10:54 172.27.4.104 166.160.133.71 TRKY HILL - MOOSIC #273 3368 BIRNEY AVE MOOSIC PA 18507 412-651-2752
pi0262 (A) Jan-16 10:52 172.27.4.108 166.160.133.69 TRKY HILL - COOPERSBURG #262 106 S THIRD ST COOPERS PA 18036 412-651-2750
pi0263 (A) Jan-16 10:52 172.27.4.112 166.160.133.72 TRKY HILL - WILKES - BARR #259 616 HAZLE STREET WILKES - PA 18702 412-651-2763
pi0270 (A) Jan-16 10:55 172.27.4.136 166.160.133.74 AMERISOURCEBERGEN 1300 MORRIS DR STE 100 CHESTER PA 19087 412-651-2755
Done
Local Intranet

FIG. 6A

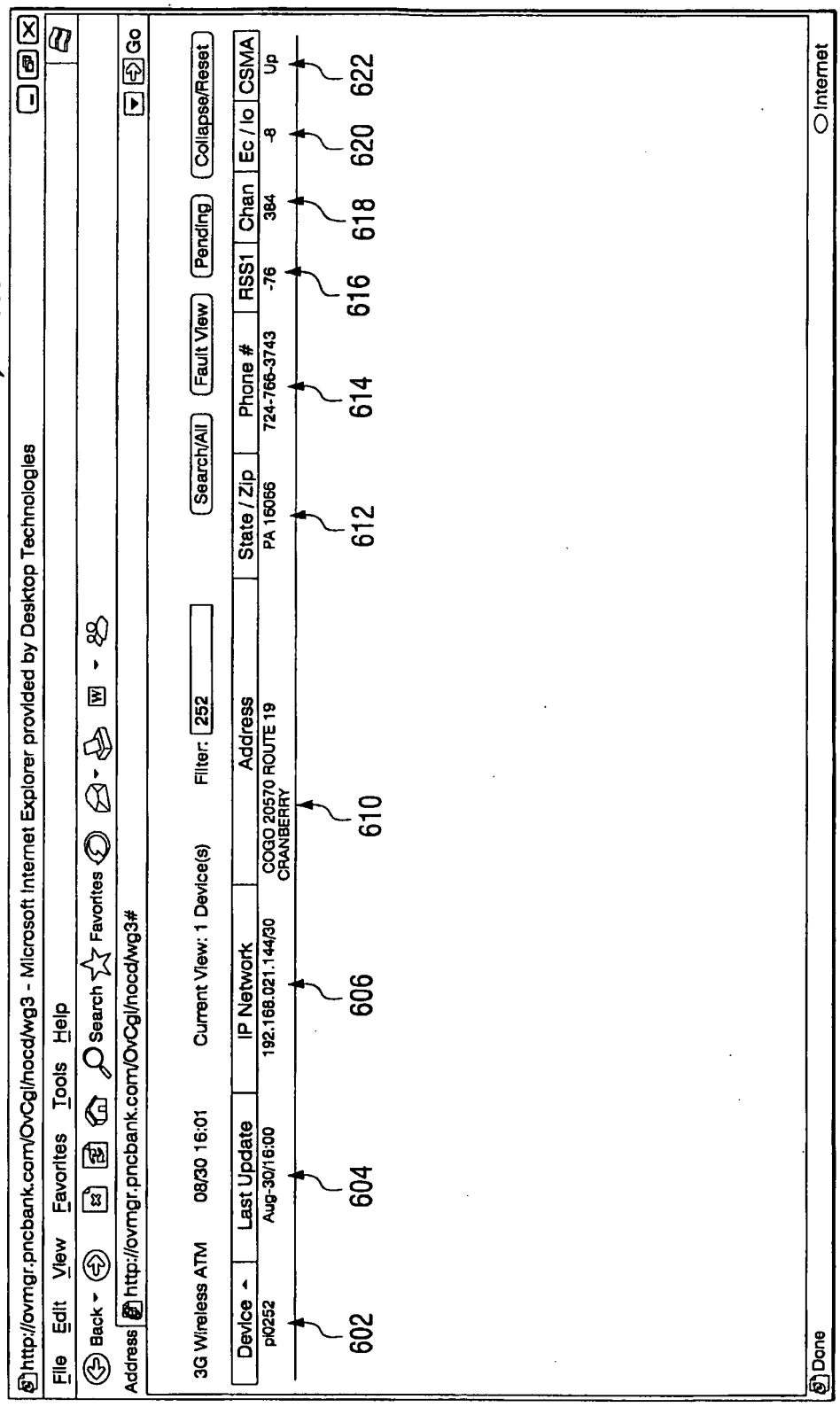

600
http://ovmgr.pncbank.com/OvCgi/nocd/wg3 - Microsoft Internet Explorer provided by Desktop Technologies
File Edit View Favorites Tools Help
Back Search Favorites
Address http://ovmgr.pncbank.com/OvCgi/nocd/wg3#
Go
3G Wireless ATM 08/30 16:01 Current View: 1 Device(s) Filter: 252
Search/All
Fault View
Pending
Collapse/Reset
Device
Last Update
IP Network
Address
State / Zip
Phone #
RSS1
Chan
Ec / Io
CSMA
pl0252
Aug-30/16:00
192.168.021.144/30
COGO 20570 ROUTE 19 CRANBERRY
PA 16066
724-766-3743
-76
384
-8
Up
602
604
606
610
612
614
616
618
620
622
Done
Internet

FIG. 7

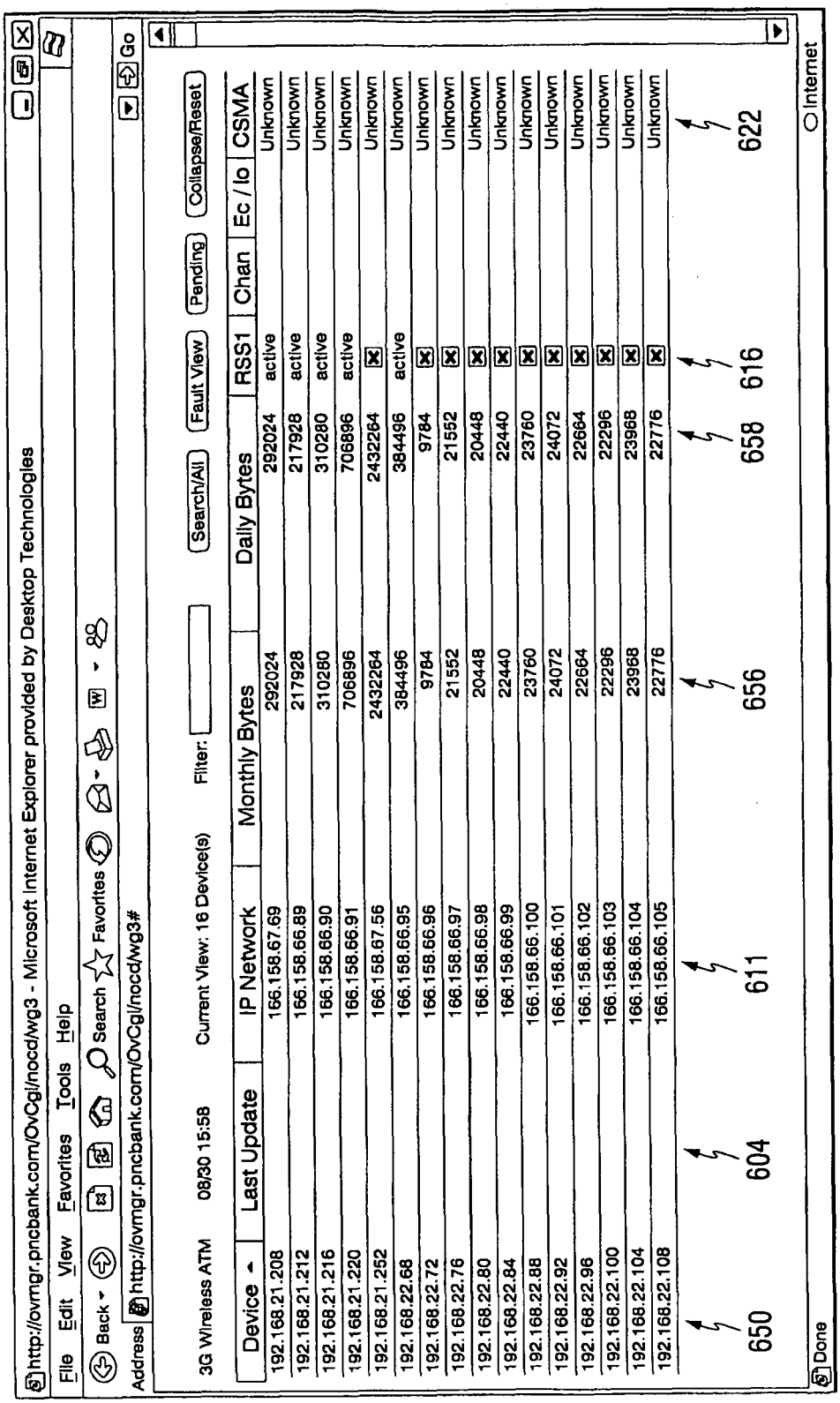

http://ovmgr.pncbank.com/OvCgi/nocd/wg3 - Microsoft Internet Explorer provided by Desktop Technologies
File Edit View Favorites Tools Help
Back Search Favorites
Address http://ovmgr.pncbank.com/OvCgi/nocd/wg3#
Go
3G Wireless ATM 08/30 15:58 Current View: 16 Device(s) Filter: Search/All Fault View Pending Collapse/Reset
Device Last Update IP Network Monthly Bytes Daily Bytes RSS1 Chan Ec / Io CSMA
192.168.21.208 166.158.67.69 292024 292024 active Unknown
192.168.21.212 166.158.66.89 217928 217928 active Unknown
192.168.21.216 166.158.66.90 310280 310280 active Unknown
192.168.21.220 166.158.66.91 706896 706896 active Unknown
192.168.21.252 166.158.67.56 2432264 2432264 Unknown
192.168.22.68 166.158.66.95 384496 384496 active Unknown
192.168.22.72 166.158.66.96 9784 9784 Unknown
192.168.22.76 166.158.66.97 21552 21552 Unknown
192.168.22.80 166.158.66.98 20448 20448 Unknown
192.168.22.84 166.158.66.99 22440 22440 Unknown
192.168.22.88 166.158.66.100 23760 23760 Unknown
192.168.22.92 166.158.66.101 24072 24072 Unknown
192.168.22.96 166.158.66.102 22664 22664 Unknown
192.168.22.100 166.158.66.103 22296 22296 Unknown
192.168.22.104 166.158.66.104 23968 23968 Unknown
192.168.22.108 166.158.66.105 22776 22776 Unknown
650
604
611
656
658
616
622
Done
Internet

FIG. 8

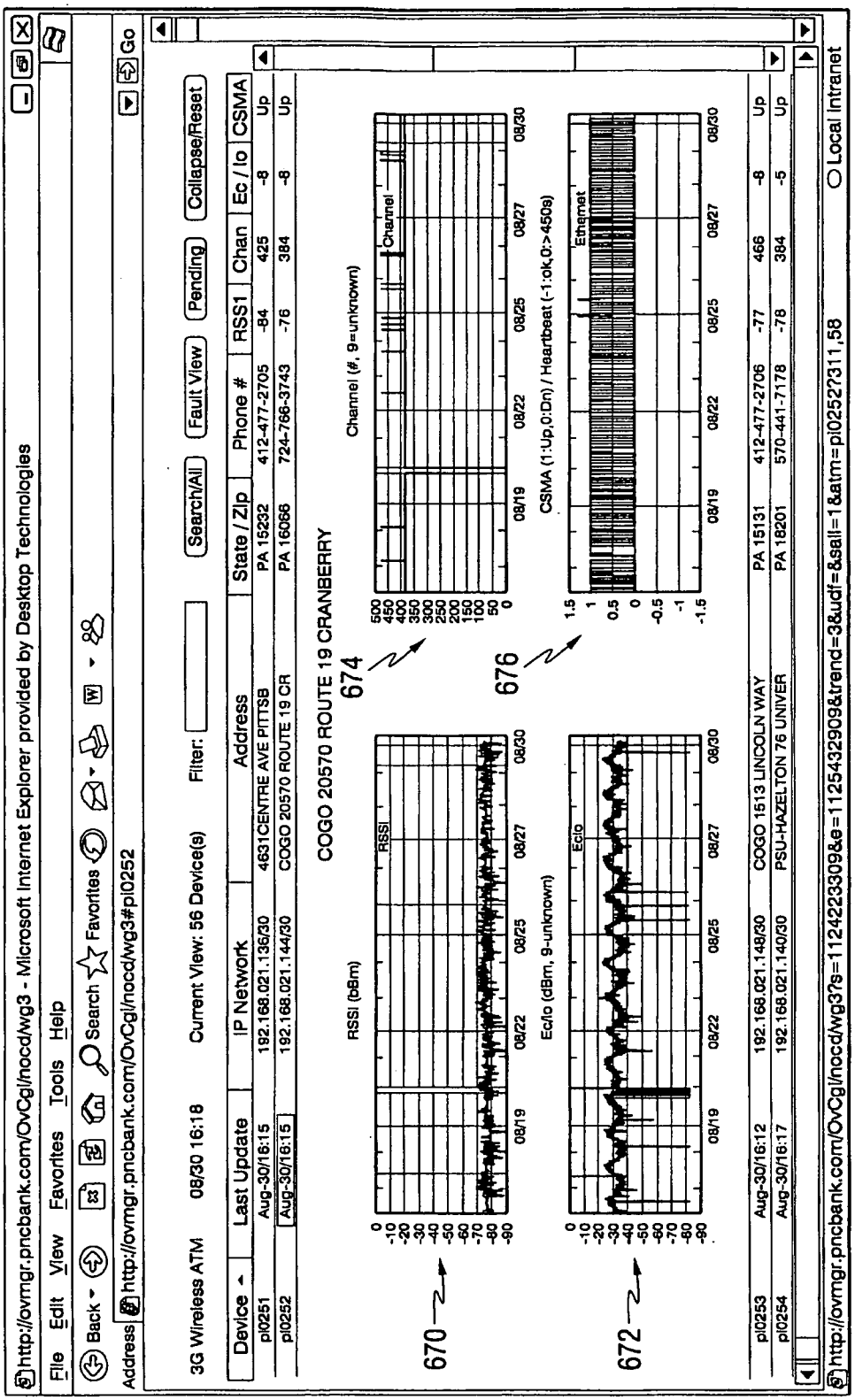
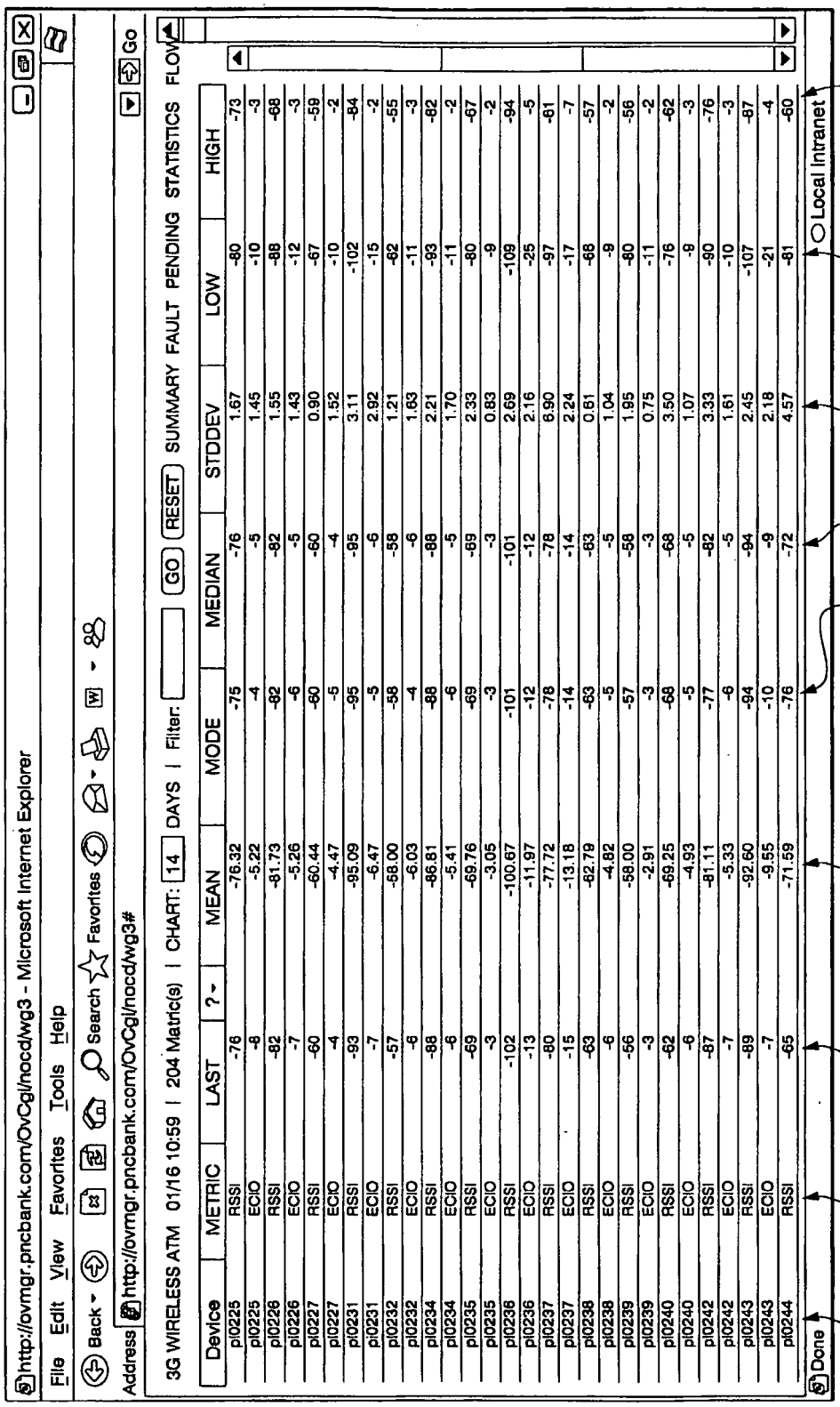

600
http://ovmgr.pncbank.com/OvCgi/nocd/wg3 - Microsoft Internet Explorer provided by Desktop Technologies
File Edit View Favorites Tools Help
Back Search Favorites
Address http://ovmgr.pncbank.com/OvCgi/nocd/wg3#pl0252
Go
3G Wireless ATM 08/30 16:18 Current View: 56 Device(s) Filter: Search/All Fault View Pending Collapse/Reset
Device Last Update IP Network Address State / Zip Phone # RSS1 Chan Ec / Io CSMA
pl0251 Aug-30/16:15 192.168.021.136/30 4631CENTRE AVE PITTSB PA 15232 412-477-2705 -84 425 -8 Up
pl0252 Aug-30/16:15 192.168.021.144/30 COGO 20570 ROUTE 19 CR PA 16066 724-766-3743 -76 384 -8 Up
COGO 20570 ROUTE 19 CRANBERRY
674
676
670
672
RSSI (dBm)
RSSI
Ec/Io (dBm, 9-unknown)
EcIo
Channel (#, 9=unknown)
Channel
CSMA (1:Up,0:Dn) / Heartbeat (-1:ok,0:>450s)
Ethernet
08/19 08/22 08/25 08/27 08/30
pl0253 Aug-30/16:12 192.168.021.148/30 COGO 1513 LINCOLN WAY PA 15131 412-477-2706 -77 466 -8 Up
pl0254 Aug-30/16:17 192.168.021.140/30 PSU-HAZELTON 76 UNIVER PA 18201 570-441-7178 -78 384 -5 Up
http://ovmgr.pncbank.com/OvCgi/nocd/wg3?s=1124223309&e=1125432909&trend=3&udf=&sall=1&atm=pl02527311,58
Local Intranet

FIG. 9



Device	METRIC	LAST	?	MEAN	MODE	MEDIAN	STDDEV	LOW	HIGH
pt0225	RSSI	-76		-76.32	-75	-76	1.67	-80	-73
pt0225	ECIO	-8		-5.22	-4	-5	1.45	-10	-3
pt0226	RSSI	-82		-81.73	-82	-82	1.55	-88	-68
pt0226	ECIO	-7		-5.26	-6	-5	1.43	-12	-3
pt0227	RSSI	-60		-60.44	-60	-60	0.90	-67	-59
pt0227	ECIO	-4		-4.47	-5	-4	1.52	-10	-2
pt0231	RSSI	-93		-95.09	-95	-95	3.11	-102	-84
pt0231	ECIO	-7		-6.47	-5	-6	2.92	-15	-2
pt0232	RSSI	-57		-58.00	-58	-58	1.21	-62	-55
pt0232	ECIO	-6		-6.03	-4	-6	1.63	-11	-3
pt0234	RSSI	-88		-86.81	-88	-88	2.21	-93	-82
pt0234	ECIO	-6		-5.41	-6	-5	1.70	-11	-2
pt0235	RSSI	-69		-69.76	-69	-69	2.33	-80	-67
pt0235	ECIO	-3		-3.05	-3	-3	0.83	-9	-2
pt0236	RSSI	-102		-100.67	-101	-101	2.69	-109	-94
pt0236	ECIO	-13		-11.97	-12	-12	2.16	-25	-5
pt0237	RSSI	-80		-77.72	-78	-78	6.90	-97	-61
pt0237	ECIO	-15		-13.18	-14	-14	2.24	-17	-7
pt0238	RSSI	-63		-62.79	-63	-63	0.61	-68	-57
pt0238	ECIO	-6		-4.82	-5	-5	1.04	-9	-2
pt0239	RSSI	-56		-58.00	-57	-58	1.95	-80	-56
pt0239	ECIO	-3		-2.91	-3	-3	0.75	-11	-2
pt0240	RSSI	-62		-69.25	-68	-68	3.50	-76	-62
pt0240	ECIO	-6		-4.93	-5	-5	1.07	-8	-3
pt0242	RSSI	-87		-81.11	-77	-82	3.33	-90	-76
pt0242	ECIO	-7		-5.33	-6	-5	1.61	-10	-3
pt0243	RSSI	-89		-92.60	-94	-94	2.45	-107	-87
pt0243	ECIO	-7		-9.55	-10	-9	2.18	-21	-4
pt0244	RSSI	-65		-71.59	-76	-72	4.57	-81	-60

FIG. 9A

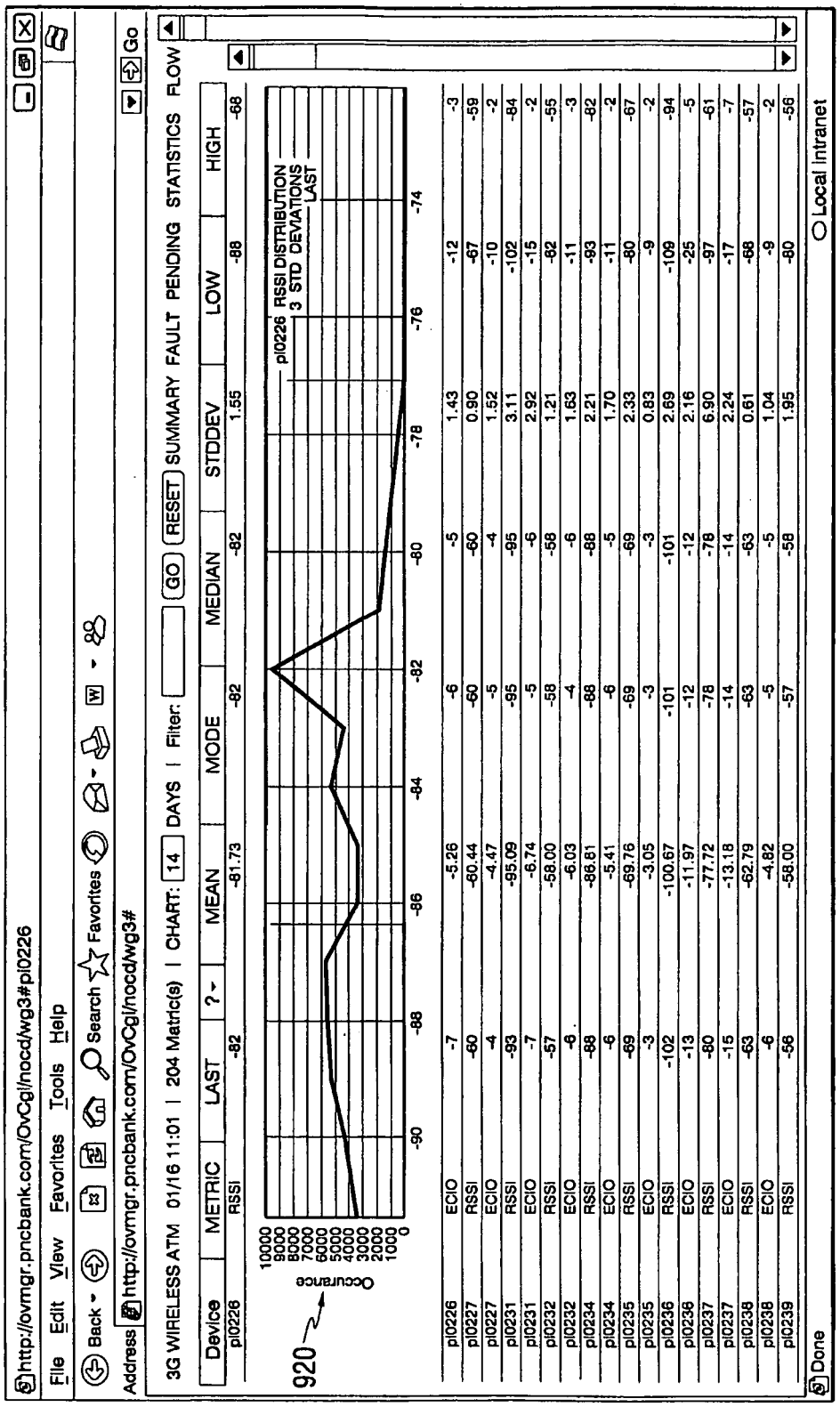

http://ovmgr.pncbank.com/OvCgi/nocd/wg3#pl0226
File Edit View Favorites Tools Help
Back Search Favorites
Address http://ovmgr.pncbank.com/OvCgi/nocd/wg3#
Go
3G WIRELESS ATM 01/16 11:01 | 204 Matric(s) | CHART: 14 DAYS | Filter: GO RESET SUMMARY FAULT PENDING STATISTICS FLOW
Device METRIC LAST ? MEAN MODE MEDIAN STDDEV LOW HIGH
pl0226 RSSI -82 -81.73 -82 -82 1.55 -88 -68
920
Occurance
10000 9000 8000 7000 6000 5000 4000 3000 2000 1000 0
-90 -88 -86 -84 -82 -80 -78 -76 -74
pl0226 RSSI DISTRIBUTION
3 STD DEVIATIONS
LAST
pl0226 ECIO -7 -5.26 -6 -5 1.43 -12 -3
pl0227 RSSI -60 -60.44 -60 -60 0.90 -67 -59
pl0227 ECIO -4 -4.47 -5 -4 1.52 -10 -2
pl0231 RSSI -93 -95.09 -95 -95 3.11 -102 -84
pl0231 ECIO -7 -6.74 -5 -6 2.92 -15 -2
pl0232 RSSI -57 -58.00 -58 -58 1.21 -62 -55
pl0232 ECIO -6 -6.03 -4 -6 1.63 -11 -3
pl0234 RSSI -88 -86.81 -88 -88 2.21 -93 -82
pl0234 ECIO -6 -5.41 -6 -5 1.70 -11 -2
pl0235 RSSI -69 -69.76 -69 -69 2.33 -80 -67
pl0235 ECIO -3 -3.05 -3 -3 0.83 -9 -2
pl0236 RSSI -102 -100.67 -101 -101 2.69 -109 -94
pl0236 ECIO -13 -11.97 -12 -12 2.16 -25 -5
pl0237 RSSI -80 -77.72 -78 -78 6.90 -97 -61
pl0237 ECIO -15 -13.18 -14 -14 2.24 -17 -7
pl0238 RSSI -63 -62.79 -63 -63 0.61 -68 -57
pl0238 ECIO -6 -4.82 -5 -5 1.04 -9 -2
pl0239 RSSI -56 -58.00 -57 -58 1.95 -80 -56
Done
Local intranet

FIG. 9B

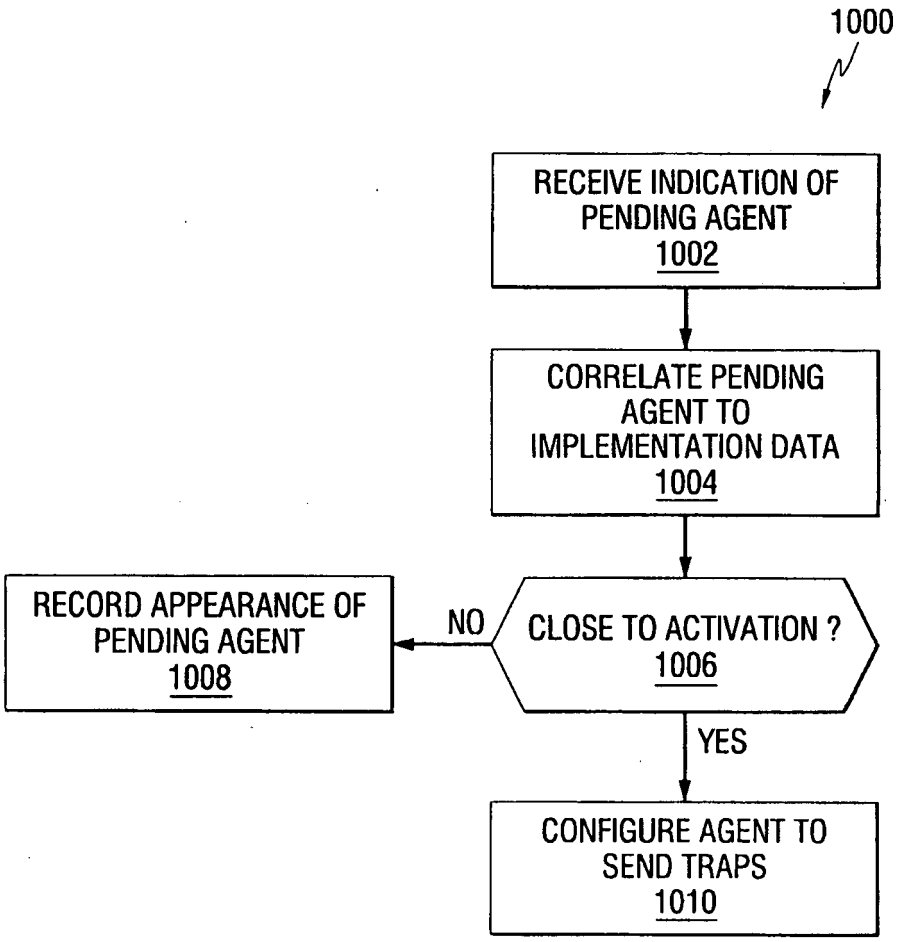

1000
RECEIVE INDICATION OF PENDING AGENT
1002
CORRELATE PENDING AGENT TO IMPLEMENTATION DATA
1004
CLOSE TO ACTIVATION ?
1006
NO
RECORD APPEARANCE OF PENDING AGENT
1008
YES
CONFIGURE AGENT TO SEND TRAPS
1010

FIG. 10

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- EP 0455402 A2 **[0003]**
- US 005651006 A **[0004]**
- US 007036048 B1 **[0005]**